FRAUD TALK – EPISODE 103

An Insider's Look at Combating COVID-19 Stimulus Fraud

Mike Ware, CFE and Inspector General for the U.S. Small Business Administration, discusses the challenges his office faced in preventing and detecting fraud affecting COVID-19 stimulus programs.

Transcript

Sarah Hofmann: Hello, and welcome to *Fraud Talk*, the ACFE's monthly podcast. I'm Sarah Hofmann, the public information officer for the ACFE. Today, I'm joined by the Inspector General of the United States Small Business Administration (SBA), Mike Ware. Thank you so much for joining us today, Mike.

Mike Ware: Thank you for having me. It's a great honor.

Sarah: Great. As everyone's lives have been affected by the COVID-19 pandemic, your role specifically as Inspector General for the Small Business Administration has become more important than ever. There have been billions of dollars given out in loans to small businesses through both the Paycheck Protection Program and the Economic Injury Disaster Loan (EIDL) Program.

Out of curiosity, what were some of the first few months like for your office right after the CARES Act was passed? I kind of assume it was a little chaotic just because of how quickly everything was happening.

Mike: Hey, listen. Chaotic might be a little bit of an understatement. No, I'm just kidding. It was chaotic for certain, but to be honest, not as chaotic as you would think in the first few months. Now, I am the eternal optimist. I'm the one with the energy that thinks that we could do it, we could do it no matter what. The staff might have a different take on this probably. I have to say that it's gotten increasingly chaotic, but not so much in the first few months. I think that was due mainly to two things that we do well around here.

One is our expertise in SBA's programs and systems. Right? This is what we do. The second is our internal planning. Ever since I came here, the emphasis on repeatable processes. As you probably know, most folks have been working remotely since, what, mid-March or something. Fortunately, we had, what I would call, a very smooth transition. That was because of the decisions we had made over the years to ensure that we had necessary systems in place.

I'll give you an example. Our mobile IT platform, our leave policies, our flexible work options… Some of these flexible work options were tweaked over the years. When I got here first, folks had one day telework. We did a pilot for two days to see how that's working out. That's what we went with. Mainly because although we have locations in 13 different states, we are primarily in DC co-located with the agency.

I want to always have a presence here, and that's why we did the two. The folks have done such a great job of being productive that we'll be even with the three whenever we get back to whatever normalcy will look like in the future. It's worked out way better than I expected.

Another thing internally, we really rallied around that internal expertise that we have. We developed a plan that revolved around getting timely information to the agency because when the money is moving this quickly, that information about what they need to do to make sure that money is safe is critical. It has to get to them real fast. We were able to do that.

Before the issuance of the first loan, we issued two reports based on our already existing body of work. Those reports were to provide them a preventative method that would address the potential fraud we knew from our experience would take place. Those “lessons learned” reports were issued at that time. I always say that it is very important that people understand that fraud prevention starts at the onset of standing up any program. Proper controls have to be in place to mitigate risk and to ensure that programs operate as intended. We all see the press releases detailing the arrests. A well thought-out system of controls goes a long way in terms of mitigating the risk of fraud. That's why we wanted to get the information into their hands quickly, and that's what our plan revolved around.

At the same time, we put out a supplemental audit plan, an oversight plan, detailing to the public and to the agency and to Congress exactly what we would be looking at. Then I'd be remiss in terms of chaotic, in terms of speaking about things that helped us in this environment, was that we were able to secure necessary partnerships with internal and external partners.

We are part of several task forces with the U.S. Attorney's offices, with the Department of Justice (DOJ), and that is one of the primary reasons that you've seen so many early arrests. I don't know. I could go on and on on this in terms of the chaos and in terms of how we pivoted, but maybe that's enough.

Sarah: It definitely sounds like you believe, and I believe and so many fraud examiners believe…an ounce of prevention is worth a pound of cure. It really sounds like you had that strong framework, that groundwork already done so that it helped in such a strange time, unprecedented times, to just make sure that that prevention was already in place as much as humanly possible.

Mike: That's something that I've found across government in terms of our approach to how we're providing oversight of these funds and in terms of how we're catching fraudsters and in terms of how we are preventing fraud. In my office and the US Attorney's Office and Department of Justice, FBI, FDIC, IRS, all these people we're partnering with, they're so committed to this task. That definitely makes it easier and it makes it work.

Sarah: That's wonderful. You just mentioned how important your relationship with your office and the different law enforcement, whether it's local law enforcement or the different agencies, how important those relationships really are. How have you fostered and strengthened those relationships, not just during the pandemic but beforehand? Specifically thinking of it from a fraud examiner’s standpoint, how important do you think it is for Certified Fraud Examiners to work with their local law enforcement with their investigations? Do you have any tips they might be able to use?

Mike: Let me start with the first part of that. How did we foster these relationships? It's a normal part of our business that we partner with other law enforcement entities because we're the Small Business Administration. The government-wide contracting goals come under us. That contracting part touches all of government. In terms of our fraud cases, we work with, particularly other offices of Inspectors General to root out fraud in these programs because it touches us, of course, as the head, and it touches everybody else in terms of their contract vehicles. Same thing in the loan programs.

We already had these relationships built up with U.S. Attorney's offices across the country and with federal law enforcement partners because we do most of our work with them. We do partner on the local and state levels across the United States. It's interesting in that, because like I said, most of our work is with the federal law enforcement partners, but many times, depending on their size… How best to put this? State and local law enforcement agencies do not necessarily have the depth of experience in terms

of working complicated fraud investigations involving government contracts, grants and other federal funding instruments.

So our auditors and special agents are seen as experts on those types of investigations because that's their bread and butter on what they do for a living. It's immediately recognized with those collaborations in terms of bringing things to the table. That's why it's important for CFEs to develop close working relationships and to partner with local law enforcement because of the expertise *they* bring to the table in their respective areas and what both sides provide to fraud investigations. For us as an office, the partnership also becomes important on the rare occasions when we want to present one of our cases to local and state attorney's offices for prosecution.

That would happen if AUSA (Association of the United States Army) has not accepted the case because it didn't meet their prosecutorial guidelines. Those state and local law enforcement agencies are used to working with their prosecutors. That provides us with invaluable assistance and guidance. We've also partnered recently… so a big part of the fraud that we're finding in these programs is in identity theft. And identity theft victims are filing reports with their local police departments. They're contacting our office to report the fraud and to gather additional information to further their ongoing investigation. That partnership has taken place as well.

Let me see. Let me get to that part, in terms of tips, we, along with the Secret Service, placed a fraud alert, and since then, that many financial institutions have used to dig deeper into fraud by recognizing the fraud trends. I could give some examples on that, and I think that would help us in terms of tips, in terms of what to look for. We ask them to look at newly created or multiple bank accounts that had what we've referred to as abnormal transaction activity.

Or, these deposits are being made to consumer accounts rather than business accounts or the money is coming in and out within like one day. Then definitely with green dot account activity and transfers to overseas accounts with this money coming in. And of course, the large personal expenditures that you read about in the news. To be honest, we've received much of those tips from fraud professionals and CFEs at financial institutions across the nation that they contacted us about what they were seeing. We were just able to put it all together in a neat package for everybody to be able to use.

Sarah: I was curious, because you were saying you're getting a lot of tips from the financial institutions themselves. Can you walk listeners through the process of, let's say that you have a case of suspected fraud related to stimulus money. What happens from start to maybe not complete finish, but from where you guys first get involved and what steps you take from there?

Mike: I have to tread pretty lightly on this, but let me see if I can not get myself in trouble.

Like you said, we're receiving reports of fraud from various sources. The financial institution had been a big part of that, but we also get referrals from the program divisions at the Small Business Administration. They are experts, of course, in their respective programs. It's also coming from federal, state and local law enforcement partners and the prosecutors. A lot of it is coming through our OIG (Office of the Inspector General) Hotline, but our data analytics unit has been excellent at identifying fraud patterns and trends. That has helped us to focus more on a pinpointed approach to investigations.

But I'll talk to you about the typical fraud case. Of course, in this case, it’s going to just about always begin with identity theft or fraudulent loan application.

You'll see false statements on applications that could run a gamut from completely making up a business to declaring that the business was in existence for years, or the submission of fraudulent supporting documents like fake payroll, fake employees, inflation of payroll. I spoke about ID theft, but this has been

major. We believe it's because of the widely covered data breaches that have occurred across corporate and governmental entities.

We're seeing a large amount of confirmed instances and have initiated focus work in that area. We're seeing everything from IP address manipulation to fake bank accounts later converted to the blue dot accounts. Of course, those processes involve a towering investigation of all those indicators. Importantly, I'd like to get this out there. At the very beginning, when the CARES Act was first put out, we partnered with the Department of Justice's Fraud Section to develop what we call the DOJ CARES Act Project.

Off the top of my head, our main coordination efforts involve the DOJ Fraud Section, the FBI, IRS, FDIC and others. Those are the ones I could remember off the top of my head, but the most important aspect of that was the sharing of the PPP data, which resulted in developing cases far faster than is normal. Because as you would know, the regular fraud case doesn't even kick off until a year or more after occurrence. Those will be what we're seeing and how we're working them out.

Sarah: You mentioned tips, and the *Report to the Nations* shows tips are consistently… Each year that the new *Report to the Nations* comes out, tips are always the number-one way and the most effective way that fraud gets caught, whether it's tips from employees, tips from vendors, all sorts of different avenues. Your office, I noticed, along with other oversight offices are strongly encouraging the public to use hotlines and other reporting mechanisms.

How much of an impact do you think that those hotlines or different reporting mechanisms, how much of an impact has it made on you catching or even just being able to have data and a realistic picture of how much fraud is going on as a result of the pandemic?

Mike: Right, right. Oh boy. All of the Offices of Inspectors General have hotlines that get information from the public. Federal employees, contractors. And that helps us to further our mission. Since we're [talking with] the ACFE… to prevent and detect fraud, waste and abuse in those programs. These tips, through our hotline, are of critical importance to the success of our ongoing and future criminal investigations and other work.

The main reason for it, when you think about it, it serves as a force multiplier, if you will, in terms of detecting fraud, and we'd be nowhere without it. The tips have been super critical to our early detection of fraud and fraud trends and have allowed us to move quickly to inform the agency in a way for them to shore up their vulnerabilities.

Just to provide you some context of what we're dealing with as an office.

We normally…I think if you added up the last year and a half in terms of hotline tips that we received the last year and a half before the pandemic, before the CARES Act, we probably had about 1,500 complaints of tips. Believe it or not, over the past five months alone, we've received over 26,000 online complaints and 42,000 phone calls.

Sarah: Wow.

Mike: The total has climbed to more than 75,000 complaints. Now, we're in a process of evaluating all the complaints. I had to reassign staff to the hotline to deal with it. We have a system that serves to identify the most critical ones, and that has been resulted in leading to the faster investigations and to the analysis of fraud schemes. It's verifying. It verifies what we're finding in terms of the data. When the data says, this is going on.

Let me see if I could provide an example. Well, you know what? I'm not sure if I could speak about that yet because that one is ongoing, so I'll hold and I'll just keep it at, it verifies what we're finding through the data.

Sarah: Speaking also, you're talking about the data and talking about the use of data analytics. I also saw that you had spoken a little bit earlier, I believe in the summer, to the media about how you've also been able to use social media in addition to data analytics, to uncover fraud in real time.

How are you using these types of tools? Is there any certain type of tool, whether it's a certain type of data analytic program or like I've mentioned, social media, what are you finding to be most effective?

Mike: Let me start with social media, just to give some context on that. What we were finding early on, the data was pointing to the fact that there were a ton of applications coming from single IP addresses, for example. There may be a reason for that, but there might not be a reason for that. As the agents and the data analytics group started to pour over social media, they were finding that there were people out there advertising their services, basically saying that the government was giving away money for real context, and they were teaching you how to go about obtaining these funds illegally.

Telling you to show up at certain places, we have 30 laptops, and all you have to do is… We'll walk you through your application process, and then they charge a fee. We started to see that on the back end when the bank started to call us to say, "When we ask a secondary question to the person who was coming to immediately withdraw the money, they have no idea what the funds were, what the source of the funds were."

They said, "Well, we were just told that if we applied for this, maybe we get to keep $8,000 and they'll keep $2,000 of the $10,000 grant, the initial grant that went out on EIDL." That really started to trip the banks, and that's when we started to work with them a lot more closely. That type of thing was going on, but in terms of data analytics, we were so fortunate that we made a case before our appropriators and Office of Management and Budget to have an investment made into the data analytics capability of our office.

This was a couple of years ago, and man, that's a timely investment because of the incoming loan data and the weaknesses that we're helping to identify in the SBA's internal controls. But the data matching tools and authorities, they have been critical for us. The way it's working, we currently use a data matching tool in coordination with the Department of Treasury or IRS data, and of course, we're analyzing plenty of data from SBA systems.

This is what has allowed us to focus on the most egregious fraud and to maximize our effectiveness upfront because, like I say, this is moving in warp speed in comparison to what normal investigative efforts look like.

I think you asked about some examples. I could talk about a case or two, because they've been pretty public. One was where someone got over $1 million in PPP funds. Upon our reviews, we found that, or the investigation found that he actually bought a Lamborghini with it, Rolex watches, and had many visits to the strip clubs, using the money. I don't think they counted as employees.

Another one, the most recent one I think we've announced, or DOJ has announced with us, is the arrest of the person that had over $6 million in PPP loans, for companies with *Game of Thrones* names. Nothing to do with saving employee jobs. Might have saved a dragon or two, but definitely didn't save employee jobs.

The data analytics function is helping to drive this type of work. They work closely with the audit teams and with investigations to help improve overall efficiency and effectiveness. Right now, it's being used to

get a higher quality audit and investigative evidence and better correlating audit and investigative approaches to risk as well. We're just at the tip of the iceberg on this. Much, much more will follow.

Sarah: I'm sure that the, I don't know if fallout's the right word, but yes, that this is just going to continue for years and years to come just with the sheer volume of data that you have to go through and the amount of money. It's a staggering amount of money that needed to get injected into the economy, but just now, taking that time to untangle everything, it'll be a while. I'm sure that you will be quite busy for quite a long time after this.

Mike: We definitely anticipate that, but we do anticipate, hopefully, that our work will result in changes in terms of the control environment at SBA that would allow, let's say, we have a next tranche of funding that comes out that allows them, let's just say, a better control environment. Yep.

Sarah: I've noticed that you've been pretty transparent. Like I mentioned, I have read articles that you've contributed quotes to since the pandemic. I know that there have been hearings. There are the reports that you mentioned. It seems like you and your office have been pretty transparent about the amount of data that you've collected, the amount of fraud that you've been seeing and having reported to you.

I know that sometimes just the perception of detection is enough to deter people from committing fraud. That's why I know we recommend making if you're working at an organization to have it be well-known that you do yearly audits, that you have external auditors come in just so that people are aware, "Hey, if I want to try and get away with something, it's going to get caught."

How important do you think that you and your office being so transparent, in this time, has also contributed to helping deter fraud or increase that perception of detection?

Mike: Exactly what you just discussed. It was what went into our thought process in terms of transparency. Transparency is one of the key hallmarks of any Office of Inspector General. I don't know who said it, but it's been said that sunshine is the best disinfectant and electric light is the best policeman. We certainly believe that here. Before the first loan went out the door, we informed the public and our stakeholders of potential fraud and scam schemes.

We issued a fraud alert before the first loan went out and published it on our website and on social media. We engaged with stakeholders such as NAGGL, the National Association of Guaranteed Government Lending, to share the fraud and scam alert broadly to SBA's lending partners. We also engaged the media. This is why we're always encouraging people to report fraud, waste and abuse to our hotline. Like I said, that becomes a force multiplier to our efforts. You also have all the press releases that continue to come.

All these days run into each other, so I believe it was three weeks ago now, that I was part of the Department of Justice national press conference where we marked the 50th arrest so far, and by the time we were up there speaking, the number was up to 57. We have imperative data that tells us that this works. I can't get into specifics too much on this, but let's just say that a secondary follow-up of suspicious actions results in many fraudsters walking away from the money.

Just a secondary question based on data and on the fraud schemes, what the financial institutions are finding in partnering with us. Let's ask a follow-up question. All of a sudden, the folks don't show up for the money anymore. That's what this light does.

Sarah: It's one of those things I feel like it seems so simple, but it can be such a deterrent. Just ask a couple of more questions and fraudsters aren't necessarily prepared for that. They think, I'm just going to do what I think needs to be done to fraudulently get this money and just… It's so interesting to me that it's that simple that turns them away.

With the potential of new stimulus money through the CARES Act or any possible upcoming legislation, I know that we're still very much in the thick of the pandemic, and I don't think that things will go right back to normal or that we won't still see negative impacts on the economies. People will still need stimulus money for probably years to come. With the potential, though, of new stimulus money, will your office be able to affect some of the control issues that arose from the initial spending in spring?

Mike: We sure hope so. That is a critical piece of what IG shops are supposed to be doing. Now, we all know, SBA was given a tremendous role in the nation's response to mitigate this economic impact of COVID-19. What we know is over a trillion dollars in lending authority was made available to SBA through public law, and in fairness, SBA has a long-standing challenge and we've written this every year — at least since I've been here — as a top management challenge for the agency. That challenge is speeding aid to people in desperate need while balancing against a proper controlled environment.

By the time you read one of our reports, by the time one of our reports is made public, there have already been many meetings with the agency with us detailing what's coming and what needs to be done right now. In some instances, SBA has done a great job pivoting to shore up those vulnerabilities, and this is what we're really after. Between those internal meetings… because some of this, the timing on it is so critical. When we find a new fraud schemes, keeping in mind that fraudsters do what fraudsters are going to do, so it's going to be new fraud schemes coming up.

When we identify them, we try to immediately notify the agency of where the vulnerabilities are so they can shore it up. Between those meetings and with our held briefings, that's the most critical way we have to affect the mitigation of fraud risk. We've seen it happen before, so I'm both hopeful and expectant that changes will be made.

Sarah: It sounds like just with everything that has happened with the pandemic that, not to say that you can predict the future and I don't think that anyone could have predicted exactly what was going to happen with the pandemic back even in January, but it seems like because of your knowledge of the importance of controls and the importance of having the data analytics tools and stuff that you were able to start in a better place when all of this unexpected stuff came out.

Not that you could see into the future, but it sounds like just from your experience, you knew how to set yourself up in the best possible way.

Mike: It wasn't like we could see into the future, but we definitely knew because SBA's disaster program, for example, as a matter of fact, and the flagship 7(a) program, they both have similar challenges. Except with the disaster program, and that's the one that covers the EIDL program, Economic Injury Disaster Loan program. That's a direct lending program by SBA, by the way.

What happens with them is that they're tasked with getting this money out to people who have suffered disasters, normally a hurricane, fires, tornadoes. This is what SBA does, so we knew what controls needed to be in place going in because of the challenges that we identified in the past. Remember, Harvey, Irma, Maria wasn't that long ago. So we knew with this much money that dwarfed by far, Harvey's, Irma's, Maria's lending authority…dwarfed it, maybe 15 times or something like that.

We knew how those problems were going to present themselves and exactly what needed to be done to mitigate the fraud risk.

Sarah: With you mentioning that you already had an idea with the emergency situation what to anticipate, are there any big lessons that you've seen so far or that you've learned during this pandemic? The sheer amount of money, the sheer amount of applicants, have there been any very shining, obvious, big, broad things that you feel like you've learned that you definitely want to keep in mind and apply moving forward, past us dealing with just the pandemic itself?

Mike: Just continuing with the discussion that we were just having, I can't say enough how important it is for a strong system of control to be in place *prior* to releasing large sums of money. We understand that speed is critical when people are desperate. We understand that. When you sacrifice controls for speed, everybody loses. It's way more work on the back end.

What we've learned and what we know, but how do you get that message across in a way that tips the scale a little bit toward the risk mitigation part? That has to be at the forefront of everyone's thinking. People feel that we can just go run after the money after it's gone. That may be true to a certain extent, but it is the absolute worst possible way to think of fraud oversight.

All CFEs know that the best to deterrent to fraud is a solid system of controls that are placed upfront. Another thing that I've learned is how critical data analytics is to us in today's environment. I would strongly recommend a wide use of data analytics here, throughout the loan application process, which assists in mitigating risk. Even once the money has been disbursed, the data analytics have continued to play a critical role to uncover the fraudulent loan applications and to provide information leading to the identification of the fraudsters and the identification of the schemes that they are using. Those are two big takeaways.

Sarah: That makes perfect sense. I feel like everything that you've just explained about tackling this. Again, I know it's a little bit overused right now, but we're in unprecedented times and it's unprecedented programs that have been needed. Trying to get a handle on that, it just seems like the main takeaway I feel like I've gotten from this discussion is just really being prepared, really having an eye on the future and being very aware of predicting weak spots or places that you could increase different controls before you actually need it.

It's like having a fire extinguisher in multiple rooms in your house because you don't want to suddenly have the house fire and think to yourself, "Oh, I need to go out and buy a fire extinguisher."

Mike: Right. In this case, it doesn't even have to be something that's so complicated. Like we were talking about earlier, one follow-up question as part of your process. If the fraud or the loan application falls into certain red flag buckets, like 250 loans processed through a single IP address, like bank accounts numbers that have been changed after it's been approved. I mean, yes, there may be a reason for that, but more than likely there’s not.

Simply ask one follow-up question. Simply have a secondary review process in place. Not that complicated.

Sarah: I feel like sometimes it's the most simple fixes that somehow elude people. They think it's much more complicated when it actually isn't.

Mike: Right.

Sarah: That does it for my questions. Thank you so much, Mike, for talking with us today. It's been really, really interesting to hear your perspective as you and your office have been tacking all these unique challenges.

And thank *you* for listening. You can find this podcast and all of the ACFE Fraud Talk Podcast on Spotify, iTunes and anywhere else you get your podcasts. This is Sarah Hofmann, signing off.