

Thomson Reuters Market Insights

A Podcast for tax, legal and compliance professionals around the globe.

Episode Title: Government agencies faced sophisticated fraud in 2020.

Release Date: February 5, 2021

Intro: Thomson Reuters market insights. A podcast for tax, legal and compliance professionals around the globe.

Gina Jurva: Hello and welcome back to the Market Insights podcasts. I'm one of your Co-hosts, Gina Jurva, attorney and manager of Market Insights and thought leadership for our corporate and government business as well. If you've listened to the show before and you've heard my voice, you know that I frequently focus on fraud and today's episode will be no different. Specifically, today I will be talking about government fraud. And as we know, government agencies have dealt with unprecedented challenges in 2020 due to the COVID-19 pandemic, and those challenges will remain well into 2021 government agencies at all levels struggled to balance getting much needed COVID relief funds out the door quickly and to the rightful beneficiaries, while also preventing massive and sophisticated fraudulent activity. I mean, indeed more than \$4 trillion in COVID relief effort was pumped into the economy since March of 2020, and millions of people filed for unemployment compensation, business loans, grants, and many other types of pandemic relief, all of which government officials had to process and distribute in record time, well, another way we will focus the show today is on our second annual fraud waste and abuse report and we're going to talk about it a little bit more today with one of my colleagues who's joining me. If you'd like to download a copy of the report, you can find the report on the Thomson Reuters Institute website. With me today is my colleague Jon Coss. Jon is the vice president in risk, fraud and compliance in Thomson Reuters Government unit. He is also the founder of Pondera Solutions, A Thomson Reuters company that offers compliance and fraud, waste and abuse detection systems to healthcare and government organization. It would not be an overstatement to say that Jon lives and breathes government fraud prevention, so Jon it is so nice to have you on the show.

Jon Coss: Thanks Gina, it's good to be here.

Gina Jurva: Jon, could you just tell us briefly before we jump into this what it is that you know you did at Pondera, which is again now part of Thomson Reuters? Give us a little background on how you live and breathe government fraud.

Jon Coss: Sure, so I've actually been working in and around government systems and government fraud for about 25 years. And in 2011 I decided to start Pondera solutions specifically to help governments identify fraud, waste and abuse in large programs and in healthcare. And we partnered with Thomson Reuters for several years. The idea was that you know Thomson had world class identity analytics and we had world class behavioral analytics. And in March of last year, just as the pandemic was beginning, we were actually acquired by Thomson Reuters. So, we really bring those two things together. The identity analytics and fraud analyst to give governments a 360-degree view of their risk and their fraud in their program. It's been a really terrific partnership.

Gina Jurva: Well, we are lucky to have you with us and then you know interest in talking with about that you know, we're doing this fraud, waste and abuse report. This is our second annual report and, in this

report,, we surveyed over 100 government officials really at all levels of state and local government who are in the fraud prevention and detection space. You've had a chance to review the report. What are a couple points that stood out to you, especially with the pandemic being this over this last year in 2020 and what really stood out to you from the report?

Jon Coss: You know, I tell you, I had no idea what to expect because it's just been such an unusual year, but one thing I'd say just really, really jumped out me is that 93% of the respondents, almost all of them feel that fraud, waste and abuse will stay the same or even increase in 2021, and to me that's just amazing. I mean, considering we pumped \$4 trillion of aid into this into the country this year and the amount of fraud that's been reported, it's just been huge, and you know to think that despite all of that in 2020, most of the response to the survey feel that it's going to continue or even increase in 2021 is incredible. Also, I guess I'm surprised, but also really appreciate the realism of that response. I mean, as I said before, I've been doing this for about 25 years. I've never seen anything like it and now 93% of the people I work with say I'm going to see it again this year and they're probably right, so wow.

Gina Jurva: Absolutely, and I think you know we've talked about this at the Thomson Reuters Institute. You and I have done webinars on this and I know it's coming from so many different areas. We've seen international crime groups as a part of this type of fraud. We've seen domestic criminals going after pandemic checks, what advice could you offer?

Jon Coss: Yeah, you know I really feel for my colleagues and unemployment insurance agencies and employment departments around the country. In my opinion, there was really no way they could have been, you know, completely successful. And both you know processing new claims and also addressing fraud, waste abuse this year. When you think about it, I mean, they had 10 to 15 times the number of their average claims coming through. They were forced or, you know, I shouldn't say force, but they were asked to handle the PUA or pandemic unemployment assistance program which gave aid to Americans that were self-employed. And this is these folks usually aren't able to access unemployment typically so it was a new program, huge volumes, and these sophisticated fraud rings that came in with new ways of creating synthetic identity, stealing identities. There was no way that they can both get through their claims logs, and you know, address the fraud waste abuse problem. What's really heartening to see, though, was that Department labor stepped in, they provided \$100,000,000 of initial funding to the State Department to start to increase their technology and their ability to work through these backlogs and to address fraud, waste, and abuse. In the last few months, we've just seen tremendous improvement there, so, and the improvements come from automation and technology and then just a whole bunch of really hard work and elbow grease for the people that are on the front lines.

Gina Jurva: Absolutely. I mean, was there anything else about the report that was a surprise to you? I mean, is this really kind of what you had expected to see?

Jon Coss: Yeah, you know, given what you know, we just talked about, I think probably one of the things that really surprised me most was that 50% of respondents still said that they felt confident, are very confident that they have the tools and resources to prevent fraud. And you know, almost that many number, just about half, said routine checks that are built into their systems and processes for identifying fraud. This, despite everything that we've seen in the papers and, you know, with our customers over the past year. And you know what? This really tells me is that government agencies believe that they are being successful in the fight against routine fraud, and I think they're probably right. Most of them, and the systems, whether it's unemployment or other programs, have checks that

can identify and even prevent a lot of forms of fraud, but you know, given what we saw in the past year, I think it suggests that you know these increasingly sophisticated and professional fraudsters are really flying under the radar of the some of these programs. It might be more accurate to say they've developed some, you know, pretty sophisticated stealth technology to avoid it altogether, right?

Gina Jurva: Sure.

Jon Coss: You know, this is something that I think governments really have to, you know, become more aware of and really address going forward. It's that these bad actors are testing the systems that are in place to stop them and then they spend all day everyday finding new ways to defraud the programs. And if we don't keep up with them, we're going to continue to see these increasing fraud trends and success on the part of bad actors. As you know, we see spikes in in claims like we did in the last year.

Gina Jurva: Right and I don't think it's an overstatement to say though that so many of these people that are committing these type of crimes, this is basically their full-time job, like, they can spend, you know, large amounts of resources, time, energy, effort in doing this and so, governments unfortunately only have a finite amount of resources, and that's something, you know, with a myriad of challenges that we see in fighting fraud, including those budgetary restraints, how would you recommend that officials or administrators can optimize the way they're fighting for it? I think you mentioned technology a moment ago, but what would you recommend?

Jon Coss: Yeah, you know, I think at this point it's pretty clear that a lot of government agencies were just outgunned last year when it came to fighting fraud. It's just that plain simple. You know, as you said, the bad guys they're spending their time and their energy, and in many cases money to defraud the programs. And it turns out you know, at least in this past year, was pretty clear that they were spending more than we have. So, I think there's really a couple of things that are really important. One is that state legislatures, federal government really have to make it a priority to invest in systems to help department government agencies identify fraud, waste and abuse. And I think this really brings two things. One is that, you know, we'll bring more integrity to program fewer funds will flow to bad guys, but the second thing is by having the confidence that they're taking fraud out of the program, they'll be able to process the, you know, the legitimate claims more quickly, so we won't see the backlogs where we saw a lot of folks that were in need and qualified for aid and they still had to wait for it. The other thing I'd point out is I do think that governments still tend to, in many cases, act in vacuums and we really need to start sharing with each other what we're seeing and what we're doing to fight against fraud, waste, and abuse. I mean, fraud has to start somewhere, and if it starts in one state, in one program and then the war gets disseminated to other States and programs that there's a new fraud method and here's a way to fight it, I think will be a lot more effective in in fighting it. The bad guys are using the dark web to communicate on where they're being successful and how, and I think we need to really fight fire with fire in that case.

Gina Jurva: That's so true, having the partnership and the information sharing is really key because, like you said, if something is happening in one state the likelihood it's going to happen in another state is relatively high, because I think these are equal opportunity fraudsters in some ways.

Jon Coss: Absolutely true. You know, we talk about all the time that fraudsters don't see state lines and

then see program lines. And you know rarely will they, for example, create a fictitious business just to defraud one program in one state. They're going to take that and they're going to soak as many programs and as many states as they can until they get caught.

Gina Jurva: Right, I think like crime is not - we've seen this over and over in the past decade that crime is increasingly global, or at least borderless. In this case, we're talking about States and, you know, fraudsters definitely don't see those lines because there's opportunity, there's money to be made at the expense of taxpayers and those who really deserve the money who are in need of it and that really is the challenge, but when you're when you're monitoring when you're doing these investigations and you know you're using tools, I know in the report by the government some of the agencies reported back that they are increasingly relying on social media to monitor eligibility changes in populations, and I think in the report indicated that social media monitoring doubled from 13% to 26% in the most recent reports. So, first of all, could you talk a little bit about when we're saying monitoring for eligibility changes in populations? What does that mean? And is that an efficient way to monitor fraud? Or might there be a better way? So, that was kind of a three-part question.

Jon Coss: Yeah, I was well, I'll try to remember all three parts, but I will start by saying this one surprised me a little bit too. You know when we're talking about using social media for either eligibility changes or for finding fraud in first place that literally means that people are going out and scouring social media site to see if there might have been changing where somebody lives or a change in family composition, or anything else that might indicate you know that they should, you know, be eligible for benefits, no longer eligible for benefits or even a change in the amount of benefits. So literally going in and looking for things like that.

Gina Jurva: So just to clarify that even further, so having an investigator go on Facebook of somebody who is claiming benefits and seeing if I don't know, for instance, they're driving a Ferrari, right? Like we saw that in some of the pandemic relief where people were spending the money on expensive cars or something. So, something like that, right?

Jon Coss: Yeah, I think that's exactly right. I mean, it could be Facebook or Twitter or YouTube or any of these other social media sites. And you know sometimes it's for, you know, individual things about those particular actors. And I guess the good news is that even fraudsters sometimes can't help but brag about themselves on social media, but they could also be looking, you know, for links and networks through social media connections and communications and, you know, I think part of this increase just comes from the fact that using social media to identify and prosecute fraud has really led to some pretty big headlines. Some of the examples that you use, you know, criminals that are posting videos of their crimes or even music videos bragging about their fraud schemes and you know, in reality, I think that social media can help with some of these individual types of investigations, but it's really difficult to use on larger scale issues for a lot of reasons. One is, it tends to be more of one-off lookups on individuals. And the other obvious one is that it can be unreliable and incomplete, and I can create a social media account and claim to be somebody else. So, it's really, really difficult, you know, I think I'm summarizing here, but I think one of the other possibilities is that social media is just one of the only tools that some agencies have at their disposal for fighting fraud and you know it really in my mind pales in comparison to some of these leading technologies being able to use machine learning and other advanced algorithms to help find anomalies and expose fraud on a larger scale. So, going forward, I think it will be

part of the answer, but I really don't think it's the silver bullet that a lot of people would like to think it is.

Gina Jurva: I mean the other the other thing too is most respondents to the survey as we talked about a moment ago, they agree that fraud is going to increase or stay the same in 2021. I mean, really, it's the outlook is not great in terms of fraud, stopping fraud. But with that in mind, I mean would an emphasis on fraud prevention versus the detection be a more ideal way to stop fraud in the first place. I mean, well, I mean, what would be some of the barriers to even having the emphasis be on prevention at the forefront instead of chasing the money later, which you often don't get back, which agencies wouldn't be able to recover?

Jon Coss: That's right, so the old paying chases they caught in the industry and this is kind of the age-old question isn't it? Is this really a game of detection or is it a game of prevention? And I also notice in this survey that there's a desire to move more efforts to prevention from detection, and actually in the 2019 surveys I went back and looked at that, and then there was a little wish to spend less time on prevention. So, I think COVID changed all that. You know, it really forced people to look at "OK, what do I do to shut the front door to fraud?" And I think it makes a lot of sense, but just practically there's just a number of barriers, especially for government. And doing this the first, I think, is that government programs for really good reasons have a very low tolerance for false positives. If they try to shut the front door on fraud, and they wrongly deny benefits to someone that you know is entitled to home and is counting on the consequences can be really big and this isn't like when your credit card is cut off because they see suspicious spending and then you have to call in and say, "Oh yeah, that was my charge" and they said "OK, we turned your credit card back on." That's not what government does. So now we're talking about if somebody gets denied, you know, they don't make a house payment, or they can't feed their family and it's just very, very dire. So, they deal with that. And then the second, I think really equally important one is this whole digital divide issue and it's really easy for us to say like looking back on COVID for example, that people should have to prove who they are by displaying identification through an online call, you know, when interacting with someone or by traveling to an office. But you know, the reality is that's easier for some of us and others. And I don't think anyone thinks it's right that someone should be able to skip to the front of the line for benefits because they have easier access to transportation or the Internet. So, this sort of, you know, balance between prevention, shutting the front door and detection of maybe some bad actors that did get through the system I think is going to be the story that will continue on into the future until we're really able to grapple better with these issues. But certainly, technology allows us to move a lot more to the front than to the back.

Gina Jurva: Absolutely, and I think that you're exactly right is how you want to make sure that the benefits are getting to the people who truly need it and as you said, the false positives. It isn't like just saying "Oh my credit card, can you turn it back on?" you know, people rely on money for a myriad of things, food, housing, clothing, etc. So, this is really important stuff we're talking about, and I think you know, hopefully there is going to be a little more emphasis on the prevention though and using that technology to make sure the bad guys don't get through.

Jon Coss: Yeah.

Gina Jurva: Well Jon, any final thoughts on the report on the outlook of fraud, waste and abuse as we go into 2021, any final last words on that?

Jon Coss: Yeah, you know, I've been thinking about this report a lot and some of the results to me were really surprising, I shared with you some of my thoughts on that, but after thinking about it, it's more a little reflection I'm wondering if I should really be all that surprised and what I mean by that is that these government frontline workers they fight the good fight every day and I'm not just saying that these are people that I work with, these are colleagues and friends. I know how hard they're working to fight fraud and these and you know, address these ever-improving front techniques. And while most of them are doing a really great job, I think a lot of their efforts frankly are targeted at more known fraud trends and many of those unknown, newer methods that are being developed, whether, like you said, are being developed here or overseas are going to continue to prosper unless we address them through technology. I mean I liken this to a very high stakes game of whack a mole where you know bad actors are testing your system when you whack him, they just pop out of another hole and that new whole includes a bunch of thought and effort and money and sophistication in order to be successful. And you know to my mind, the proof of that is in the numbers we're seeing, you know, when we're talking about, you know, more than \$30 billion in UI fraud and in the past year, for example, what's been happening in the PPP program. And finally, I know that as a technologist I'm biased, but I just don't see any other viable way to fight this. Then with increased funding and just as importantly, adoption of some of these modern fraud prevention systems, you just can't scale up people fast enough or, you know, have the funding to do it when the fire starts like COVID and you know before COVID it wasn't as big, like the housing crisis. And I don't you know that drives spikes in unemployment and other programs. I don't know what's next, but there's going to be a 'next' and we just can't keep bringing a pillow to a gunfight. If we do, we're going to lose and you know, I'm encouraged to see federal government state legislatures start to address that and you know, arm up our side with the tools they need to fight this going forward.

Gina Jurva: Absolutely, to stay as you know we, I think the one great equalizer we will have is technology, so I agree with you on that. And thank you for your thoughts, Jon. Jon Coss is the vice president in risk, fraud and compliance at Thomson Reuters Government unit. Jon, pleasure to have you on the show.

Jon Coss: Thank you, Gina.

Closing: Thank you for joining us for Thomson Reuters Market Insights for more data driven analysis of today's professional services market and in-depth conversations with industry thought leaders, please visit us online at legalexecutiveinstitute.com or blog.thomsonreuters.com or subscribe to this podcast on your favorite podcast platform. You can also follow us on Twitter at legal executives and LinkedIn under the Legal Executive Institute. Thomson Reuters Market Insights is a production of Thomson Reuters. Copyright Thomson Reuters 2020.