Thomson Reuters Market Insights.
A podcast for tax, legal and compliance professionals around the globe.

Episode title: What a new report says about fighting government fraud during the pandemic and now

Release date: June 22, 2022

Gregg Wirth: Hello and welcome to the Thomson Reuters Institute Market Insights podcast. I'm Gregg Wirth, Journalist and the Content Manager for the Thomson Reuters Institute. Today we'll be discussing the recently published Thomson Reuters Fraud, Waste and Abuse Report. An annual report that looks at how state and local governments are preventing, detecting and investigating potential fraud, waste and abuse of government resources. With me is Jon Coss, Vice President of Risk, Fraud and Compliance at Thomson Reuters. Previously, Jon was the founder and CEO of Pondera Solutions, which Thomson Reuters acquired in March 2020. Jon has spent more than the last two and a half decades working with government agencies to improve their operations and their decision-making processes through the use of analytics technologies. Welcome, Jon.

Jon Coss: Thank you, we're glad to be here.

Gregg Wirth: Great. The latest Thomson Reuters Fraud, Waste and Abuse report notes how state and local government workers the group that is the main investigators and detectors of government fraud and waste are now dealing with several challenges as they emerge from the pandemic. How would you assess the state of these critical workers at this time?

Jon Coss: I guess I'd start by saying, unfortunately, really not a lot has changed since the beginning of the pandemic. It's pretty clear to me that most program integrity professionals, these investigators, know what needs to be done. For example, using technology to move from more reactive paying chase to more proactive prevention. But they still don't have the funding to accomplish these goals and their departments overall still prioritize efficiency and service delivery over this fraud prevention issue. And I believe that program integrity shouldn't be viewed as sort of a separate or discrete function, but rather you know part of the overall goals of the department.

Gregg Wirth: Well, that's right. The report notes there's several different ways that government agencies identify fraud with the vast majority doing so through cross referencing databases within the state. What are the other ways agencies are detecting fraud today?

Jon Coss: Yeah, first of all, I'd say that the response really disappointed me for a couple reasons. The first is that criminal fraudsters know that this is a typical technique. Just checking against current state databases, so they only have to get slightly more sophisticated to circumvent these methods. For example, we saw a large number of inmates applying for unemployment insurance benefit during the pandemic, inmates. But rather than applying in their own state, they applied to other state programs so they were smart enough to know, basically, that their own state might cross match against the Department of Corrections Records. The second reason this response to this point is that fraud rings operate across states, so by simply checking within your state program against your own state records, you may be able to stop some fraud, but those same criminals are often using those same IDs in other states and will be able to continue to operate in those states until those states stop them. Then this problem was it was also reflected in respondents deprioritizing deep dive investigations, which was one of the questions. So, those types of investigations could potentially uncover cross state cross program

fraud rings, but government unfortunately still work in siloed environments, which is reflected by this cross matching of just their own state records. With all that said, I think the most important new methods that state can adopt is incorporating new technologies like artificial intelligence and machine learning into their processes. And I think about 25% of the respondents, met respondents, mentioned that, but to me, that's still surprisingly kind of low, and I can't even imagine how states could have been successful delivering services and fighting fraud over the past couple of years during the pandemic without modern technologies, it's just too much for human beings with simple technologies to address.

Gregg Wirth: Well, that makes sense and you brought up the pandemic and I know the report mentioned the impact of the pandemic on both the government agencies and on the prevalence of fraud, the report may mention that quite a bit. What were the major developments in fraud and abuse during the pandemic, as well as in the ways it was investigated and prevented?

Jon Coss: Yeah, there were so many new developments in fraud technique. It's almost impossible to list them off, but it's really clear and it became clear throughout the pandemic that criminals haven't just been sitting around and they're not continuing to use the same old techniques. They dramatically improved their capabilities and that became clear during the pandemic. So, we saw dramatic improvements in the creation and use of synthetic identities, for example. We saw massive increases in stolen identities and also the use of the dark web to trade in them and in traffic in them, that often was accompanied by even state by state “how-to” kits on how to defraud a particular program and oh, by the way, here are the identities that you need in order to perpetrate this fraud. We also saw just a large uptick in the use of technologies like IP spoofing software, bots e-mail wild cards. And then in just more basic technologies like using for sale houses or, you know, abandoned houses to have delivery toward and using mules. So, they really were ready and it's clear that they were honing their techniques, fraud often as sort of, you know, something that that increases, give it based on opportunity. It's a crime of opportunity, if you will. But in this case, it was clear that this was a case of that opportunity being met with pretty good preparation as well. What you know, the detection methods we've seen some evolution certainly even in the last couple years I think it's accelerated in some areas. That, I think the use of AI prediction algorithms, both offered by vendors and vendor driven, but even an uptick in some programs hiring more in-house data analytics, data scientists, we saw that quite a bit, and I think that's a positive trend. We also saw more use of public records data to check on claims versus, uh, reliance like we talked about before, or single state data from a Department of Corrections or Vital Records or something like that. Public records will go deeper, but it'll also go broader so it'll go cross state, cross program and can be much more effective. I thought it was interesting in the survey that Google was still the number one tool cited to support investigations that, it's not built for that. It can be effective for that, but I imagine that it poses a lot of challenges to investigators, just like any of us have challenges on Google day to day. We saw more of a willingness, maybe out of necessity, but a willingness nonetheless to take pauses and claims processing when fraud was just overwhelming the system. I've never seen that before. For a state program to actually say, and admit, we're being overwhelmed by fraud, we're going to take a slowdown in a pause and actually processing new claimants in order to make sure that we're sending money to the proper people as opposed to fraudsters. That's pretty extraordinary for government. Hopefully nothing that will have to happen again, but I think it shows the size of it. And then, finally, I'd certainly be remiss if I didn't point out that we also saw increase adoption of some more controversial techniques. Things like facial recognition software. And I think we, as a whole, whether it's government or the vendor community, weren't really prepared for some of the questions that that

brings with it in terms of privacy, bias and analytics, trust in government and the whole host of other things. So, I feel like in many ways we've compacted 20 years of new techniques and learnings into two years, and it will be really interesting to see over the next couple of years what sticks what needs to be changed, and you know what just really leaves this landscape.

Gregg Wirth: That's very interesting. It makes me think looking ahead over the few years like you suggested, you know, the report cited several challenges that survey respondents had identified that they would be facing in the future. What do you think are the most significant of these and how would they be best addressed?

Jon Coss: Sure, happy to talk about some of that, and even before I do, I think it's really interesting that 53% of the respondents, over half, expect fraud to increase over the next two years. And this is, you know, presumably going to be post-pandemic years, and I think that's really remarkable. I think it's clear to them, as it's clear to many of us that the success that some of the fraudsters had in these programs over the past two years can't be replaced easily in something else, so they're really going to keep coming back and keep hitting these programs even after the pandemic and things aren't going to return to, and I'm using my finger quotes here, but to “normal”. We're in for an interesting period of time. And I think that a couple of the biggest challenges really sort of jumped off the survey results to me. The first is that we really need to prioritize program integrity within these government programs. And it's still seen as a little bit more of a redheaded stepchild, if you will, with as I mentioned before this priority to deliver service and to service the public and keep them happy and program integrity is off to the side. And that just is a huge concern and can lead to obviously a really target rich environment for fraudsters. And then the second is that they really still continue to lack the funding to put these systems in place and why that is, I'm not sure. I think there is some reticence on the part of politicians to fund systems that may get in the way of processing claims, may slow things down, or may even lead to some false positives. I think we can look to the commercial sector that does this for some lessons here and for example, literally this weekend, my credit card, I got some alerts, and they declined some charges. My wife was trying to buy me a birthday present, and we got a fraud alert. Well, what did we do? We didn't have to wait weeks or months to remedy the situation. We just called the number on the back of the card said that the charge was legitimate and then they turned that back on and that was the end of it for a false positive. I can imagine a world where it will be like that for government so that people don't miss house payments or grocery shopping because they're depending on these programs for such things, but today that's just not how it works so false positives are just so, such a terrible thing in government, you know, if they do everything they can to avoid them, and that often obviously creates an environment where fraudsters can swoop in and take advantage of it. And I would love to see that. So, this prioritizing of program integrity and putting the funding behind that, I think, are two things that are going to continue to be challenges, but I certainly hope they're addressed.

Gregg Wirth: Exactly, exactly. You had mentioned some tools that state and local government workers are utilizing to better prevent and detect and investigate fraud. Now you talked about everything from Google to more advanced artificial intelligence and other technology solutions. What are some tools, really, that that are kind of ready to be used by state and local governments, that could make a difference in their effectiveness in doing their job?

Jon Coss: Yeah, I'll probably comment with a few broad types of tools that I believe that government should look at in order to improve program integrity, and I don't think it's a one size fits all, but certainly

I think these are areas that every government should explore. The first would be tools that help them analyze and validate claimants before payments are made and that obviously was a direction based on the survey results where most of the respondents said they really want to see increases in their attention from their department. So, these tools will include things like public records, data or analytics to identify fraud indicators such as payments being made to the same physical address or the same or similar e-mail addresses. And even better is when these two techniques are combined into what I would call a data enhanced analytics. I think that's really, really important. That'll help governments move from this pay and chase model into more preventative. The second area, no surprise, is this area of artificial intelligence and machine learning. A number of the respondents, I think 1/4 of them mentioned this, and certainly this is an area that I think is just critical. It's important because criminals are constantly improving their techniques like we talked about during the pandemic, and they're not going to stop now. They're going to continually improve and to keep pace with these improvements, government needs to use these modern technologies to keep pace. Effective AI can find, for example, emerging or nascent methods. They may just show up as anomalies, but when you have enough of these anomalies they really become trends and it allows a government or even a system to take a look at it and say what's occurring here and then you can code or even deploy some of these models to help prevent these types of fraud techniques. The thing to remember here is that when government shuts down a fraud method, criminals don't suddenly become good citizens. They instead try to innovate more and find new ways to defraud the systems. You can't stop this with just by throwing additional people at it. You need to use AI machine learning or more modern techniques. The final area I would suggest and it's sometimes a little bit counter intuitive, but that I would suggest governments look at is just a more effective case management tools. We're still working with so many governments that are managing their cases on paper and on spreadsheets. An effective case management offers a number of advantages, and obviously it allows you to more efficiently manage cases to collaborate on them, to do them faster, to do them more accurately, but it also enhances reporting and really importantly, the ability to measure investigator effectiveness, which can really support future budget asks if you're able to go and say look, our data says that by adding an investigator, we're able to save the department this much money and improper spending, then it's a lot easier to go for that ask than just to go with anecdotal responses. So, those are those are three basic areas that I think everybody should be looking at and making some improvements within their departments.

Gregg Wirth: Oh, that's great. That's great, but looking at the kind of the other side of the tools issue is the talent issue. What are some proactive measures government agencies can take to improve their employees' skills in preventing fraud, waste and abuse? Is there a certain type of training or programs that that would greatly help in this situation?

Jon Coss: You know, I think there's, well I know there's a lot of what I'd like certainly in this area is industry focused groups, so within Medicaid, within unemployment insurance, within the SNAP program there are industry focus groups that are really working to disseminate new learnings and techniques to program integrity professionals. So, that's always the 1st place that I would start, rather than it being just within the department or within the state or even relying on vendors, because certainly anything that a vendor brings is going to be vendor sent, but if I can sort of get on my soapbox a little bit, one of the things I'd really like to see is an increase in this sort of sharing across governments. And when we talk about sharing across governments, often we talk about data. But I'm talking about things like techniques or new trends in fraud or successes that one state or program has had in detecting or

preventing and even the failures. A lot of these failures because governments, like many of us reticent to talk about when we fall down, by not sharing it, it just means that there if you take a state government, for example, we're given 49 other states the opportunity to make the same mistake that we do, and that only helps fraudsters. So, I think it's really interesting to imagine a world where government investigators could collaborate, learn from each other about fraud methods, techniques to prevent it, and just general lessons learned. It's almost like a clearinghouse, and this would go cross program and cross state. We're starting to see a little bit more of that, but I think the pandemic and this huge increase in fraud has just highlighted the need to be even more effective at that, so that's my hope for the future. I don't think it should be that difficult. I'm not talking about sharing data across states or anything that has to do with privacy, but really more focusing on some of the techniques, some of the lessons learned, you know some of the some of these processes that might help and be more effective.

Gregg Wirth: Well, that's great. I really appreciate you talking to us on this today. Just looking at the Fraud, Waste and Abuse report, is there anything else that stuck out to you that you feel to mention?

Jon Coss: I think the thing that really was interesting to me was that a lot of the techniques remain the same, pre-pandemic, post pandemic and this is after literally hundreds of billions of dollars have gone out. And at first I was surprised by that, but then as I read the survey, I guess I shouldn't be because number one all of these professionals have been working very, very hard over the last two years, focused on actually addressing those discrete and individual issues of fraud. So, they really haven't had a chance to step back and say what else can I do going forward. Then the second issue has been that the federal government has been slow to fund any types of dramatic improvement, and my hope would be that that funding comes in place and going forward we're able to offer these professionals some more advanced tools and techniques to really do their jobs. And finally, one of the concerns that I do have moving forward is that, there's has been when they talk about funding, this move to modernize systems as a whole, and my concern there is taking unemployment is that if you modernize the underlying system and a government hires a third party vendor to do that, there's been a trend to start thinking well, maybe that's who we should also have modernize our fraud, waste and abuse program, so the same vendor. And this is the fox watching the hen house that we've seen in the past where really, the priority of that vendor is always going to be on more efficiency in processing claims, whether it be medical claims, or unemployment insurance claims, and the byproduct will be that fraud, waste and abuse. We saw that in the survey results. I've seen it in the past and I grow a little bit more concerned that that we're going to go back to that as our new normal, going forward. And that's something I think that we should all be careful of.

Gregg Wirth: OK, well again, thank you so much. We've been speaking with Jon Coss of Risk and Compliance at Thomson Reuters about Thomson Reuters' new fraud, waste and abuse report. Thanks very much, Jon.

Jon Coss: Thank you.

Gregg Wirth: And thank you for joining us today on the Thomson Reuters Institute Market Insights Podcast and for continuing to listen. Bye now.

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 thomsonreuters.com/institute. You can also follow or subscribe to this podcast on your

favorite podcast platform. Follow us on Twitter @TRIExecutives and on LinkedIn under the Thompson Reuters Institute. Thomson Reuters market Insights is a production of Thomson Reuters. 