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

Episode Title: The power of reporting a scam

Release date: May 4, 2021

Gina Jurva: Welcome to our Market Insights podcast, I'm your host Gina Jurva. Today's episode is part of the Thomson Reuters Government Influencer Series. A series of webinars and podcasts designed to spotlight top government officials and influencers and the work that they do to promote transparency, advanced innovation and technology, combat fraud, waste and abuse about efficiency and effectiveness in vital government programs. This episode is about tracking government fraud trends from 2020. So, every February, the Federal Trade Commission releases the Consumer Sentinel Network data book or the prior year. So, here we're talking about 2020. As we've talked about several times on this show throttles up last year at unprecedented levels, in part due to the pandemic. The FTC or Federal Trade Commission reviews millions of Consumer Reports. Those that are received at the agency and those from various law enforcement agencies that they work with, including federal, local, state and local. They are sorted into 29 top categories. So basically, this is aggregated information about what consumers told the FTC and law enforcement last year about fraud complaints on a range of full range of fraud, identity theft, and other consumer protection topics. You know this report, it helps identify broad trends that assists law enforcement and AIDS, and preventing similar fraud. Well today I'm joined by Daniel Kaufman. He is the acting director at the Federal Trade Commission's Bureau of Consumer Protection. He's going to explain the report and its findings. I will then be joined later in the show by my colleague Amanda Houston. She's the senior director of solutions and fraud risk and compliance at Thomson Reuters, and they're going to talk about really what these findings mean to government clients to consumers and ways that we can take these learnings and apply them to the future. Thank you so much for joining me, Daniel, can you tell me a little bit more about the function of the FTC Bureau of Consumer Protection, like how do you protect consumers from criminal activity like fraud and identity theft?

Daniel Kaufman: So, you know, at its core the Bureau of Consumer Protection. And the FTC is a law enforcement agency. We are a civil law enforcement agency. We don't do criminal work, but I can talk a little bit more of that later, but we go after companies that are engaged in deceptive or unfair practices that are making misrepresentations about the products or services they sell. We also went for some number of other statutes that go after sort of telemarketing fraud and statutes, dealing with privacy issues and consumer debt collection. So, the FTC does work on broad segments of the economy, yet we're a relatively small federal agency, but at its core we are law enforcement. We do a lot of action involving fraud cases where we go in, stop the bad conduct and try to get as much money as possible back to consumers. That's a really important part of our mission is to sort of stop the bad conduct, get money back to consumers and to educate consumers. We want to make sure consumers have what they need in order to avoid these kinds of scams. We've got a great website consumer.ftc.gov with a lot of very helpful information for consumers to figure out how to avoid stumbling into one of these scams and getting their money taken away from them.

Gina Jurva: It's so important, especially over this last year when we talk about protecting the consumers against fraud and really, really educating the public. We're going to get a little bit into, you know, the

types of fraud we've seen, especially as a result of the pandemic and COVID-19, but let's talk about a report that came out that really, really piqued our interest here at the Thomson Reuters Institute, and it is the FTC's Consumer Sentinel network data book. What is that report? Can you tell us about that?

Daniel Kaufman: Sure, the starting point for the report is the data that we collect, so consumers from throughout the country and internationally can file reports and complaints with the ftc@reportfraud.ftc.gov. So, we gather millions of consumer complaints and reports and annually we issue a data book in order to report back to American consumers. You know, what are we seeing? What are the trends that exist? What are the kind of complaints that consumers are making? What's the fraud that we're seeing? And I should say, we make sure that the work we're doing is timely, responsive and relevant. So, we collect all this consumer data about complaints and reports in order to inform our mission to make sure we're doing work that's responsive. That's relevant and that is addressing, you know, the issues that are important to consumers, so we've been issuing this data book since about 2008. And in the last few years we've actually been pushing out even more and more information. We issue data online quarterly, so if you are a real policy wonk and want to dig into the data, we can go to ftc.gov/explore data. And there's just so many different ways that we slice the data. You can look at it by state, by all sorts of other characteristics. So, we're trying to be as transparent as possible with the data we received, and we're also using this data to issue what we call data spotlights. We've issued a number of these every year. We were highlighting, you know, what are we seeing in the data, so we have a data spotlight recently on romance scams. You know, what are we seeing about romance scams? What should people be wary of? What can they learn about? Income scams and how are frauds happening? There was a really interesting data spotlight we did about the use of gift cards in a lot of the complaints that we're hearing. Yeah, the fraudsters are telling people to use gift cards because it's an easy way for them to get untraceable money.

Gina Jurva: Absolutely, and so with the report, the data you're saying it's consumers reporting this directly either to you or you're also getting some of the information from law enforcement is that correct as well?

Daniel Kaufman: Absolutely, you know we a lot of the complaints come directly to the FTC, but we also work with a lot of other law enforcement and private entities to get complaints. We get complaints from the Better Business Bureau from the Consumer Financial Protection Bureau from the FBI. So, we collect all of this data, put it into our database, and we share the information and make it accessible to federal, local, and state law enforcement. Then they can also sort of have the data and use it find law enforcement targets. You know it's something where it's very important we collect all the data from a lot of different sources, and we put it out there to share with other law enforcement agencies.

Gina Jurva: It sounds like a treasure trove of information, so important to follow these trends as you mentioned. How many reports of fraud, collectively, did you receive in 2020?

Daniel Kaufman: So, we do a lot to sort of make it easier for people to file complaints. And to sort of be out there asking for complaints. So, because there's an increase doesn't necessarily mean that there's more fraud happening, but of the four point 7,000,000 complaints, we got about 2.2 million we classify as fraud. You know things like impostor scams, people pretending to be from the government. 1.4 million identity theft and 1.2 million we sort of classify as “other” which can be a lot of different things. Maybe issues involving credit bureaus, banks, lenders, car issues, things like that.

Gina Jurva: And just comparing this to 2019, how did the number of reports go up? What did you see there?

Daniel Kaufman: So, the numbers definitely went up. We had a 3.2 million in 2019. In 2020, it jumped up to 4.7 million. However, although the numbers definitely did go up a lot, we're really careful to not conclude that because they went up, brought us more prevalent. Every year, we're getting more and more data contributors, so obviously when you have more data contributors giving you complete data, the numbers are going to go up and every year we're also asking consumers to file reports with us and in the past year we also launched a report fraud dot at tc.gov, specifically to make it easier than ever for people to file these reports. So, we're trying to make it easy for people to file reports so that of course contributes to getting more numbers, but you know, all these numbers are huge and they're very important to take notice of.

Gina Jurva: Sure, so perhaps it's partially that you know you you're giving people an easier opportunity like you said, like ease of access in order to report this information. And then in terms of that you mentioned a moment ago, but the top three categories of consumer fraud that you received, you said identity theft was really a big one. Can you tell us the top three again?

Daniel Kaufman: Yeah, the top three were identity theft, impostor scams and issues involving online shopping, you know could be non-receipt of goods, things like that, people order things and it is very different than what they receive.

Gina Jurva: And what was the total dollar value lost to fraud in 2020 just from the data that you have?

Daniel Kaufman: Just from the data we have, which of course doesn't count all the data we don't have, consumers reported it was a loss of $3.3 billion for fraud and that was an increase of more than, 1.5 billion from the year before, so we're talking very big numbers here.

Gina Jurva: Sure, sure, and on average just the median loss of individual consumers, and I know that there's a lot that goes into that number, but just on average, what did people tend to be losing out to some of these scams?

Daniel Kaufman: So, the median loss was $311.00, to be specific. And I should emphasize, we also want people to report these things even when they didn't fall prey to the scam. So, a lot of the reports we get are people just notifying us about it. They were able to avoid the issue, but they still are noticing it and had $0.00 in harm. But it's important data for us to have, to know who is out there trying to get money from people.

Gina Jurva: And one question I have just in terms of how it works, so when something is reported to you, let's say, a fraud scam is reported to you via the FTC website that you mentioned earlier, you mentioned you're not a criminal in a criminal Bureau, but you do civil actions. Can you just explain briefly how that would work? If I were a consumer, what should I expect?

Daniel Kaufman: Sure, we do not intervene in specific disputes, so people will file complaints with us. We get the information, we provide them back with information that we think will be helpful based upon what they've told us, but we're not going to intervene in their specific action. We just, given the volume of complaints we have, that's not sustainable for an organization of ours size, but what we do we look at that data, we look at it carefully and if we see we're getting a significant number of

complaints involving a specific entity that's engaged in, let's say, work at home scams, we'll start investigating them. So, the complaints really drive our enforcement agenda and help us look for targets that we know are affecting consumers and that are causing harm, so it's incredibly valuable and important for people to file these complaints so that we know who we need to be targeting for law enforcement purposes. And I should say, although we're not a criminal law enforcement agency, we work with a lot of criminal law enforcement agencies, and there are a lot of cases we bring that, although we're doing it civilly, eventually, criminal law enforcement will come in and go after these same targets criminally, so we are simple, but we do a lot of work with criminal partners.

Gina Jurva: And out of out of all of the states, I know the report breaks it down by state, which if our listeners haven't looked at the report yet, highly recommend you take a look at it and look at you know your individual state. I was very interested in California, which is where I'm from, but what states had the highest number of identity theft incidents?

Daniel Kaufman: So, the highest were in this odd collection of Kansas, Rhode Island and Illinois, and I don't know if you can tell me sort of what those three might have in common. I'm not sure what the answer is, but it is.

Gina Jurva: I was hoping you could tell me!

Daniel Kaufman: No, it could be they're just reporting a lot more. We're making inroads in those States and it could be something else.

Gina Jurva: And digging into the those identity theft reports just a little bit more I saw a shocking number in the report, and Amanda Houston, who I'm going to speak to in a moment, also found this number shocking, and it's about government benefits fraud. If I'm reading the report correctly, it says that that number went up an astonishing 2920%. So first I need to ask you, did I misread that number?

Daniel Kaufman: It was not a typo. It is astonishing, so it went up from in 2018. We got 23,000 of those reports 2020 we got 406,000, a huge increase and that was a very important issue for us that we had to address. Getting information out to consumers. And it was a large scam that really erupted in the midst of the pandemic, with impostors filing claims for unemployment benefits using the names and personal information of other people. And people would find out about it eventually and be very confused as to what was going on. So, if that happened to you, identitytheft.gov, we have specific information for people who were the subject of that kind of scam. But yeah, the growth in that and the explosion was really shocking. And it's also something as soon as we saw the number spiking up, we were out there informing consumers and also working with other federal partners to make sure we had a handle on the situation.

Gina Jurva: Yeah, it's something that we've done a lot of work on here at Thomson Reuters. We've been following that trend and I know that, you know, a lot of it has come from overseas. It's been international crime rings who have engaged in it specifically the unemployment benefits or the UI fraud and so the number is shocking, but I think also not necessarily unexpected, just based on everything we've been seeing it just out there in the public record. There’s another part of the report that I actually found interesting and you could maybe tell me a little bit more about it. So, you break the report out also by military fraud for those consumers who are members of the military or retired. Why is that? Is that something you've done since the report’s inception Tell us a little bit more.

Daniel Kaufman: So, fraud preyed upon to service members is an area we've been interested in for a while. We actually have a specific website for service members military.consumer.gov. Service members, like all consumers, are potential targets for fraudsters and there are some unique issues for the military community. You know, military families may be relocating, may be relocating frequently and a lot of service members for the first time are on their own and earning a paycheck. So, we've definitely seen a lot of fraud directed at the military. We wanted to make sure that we were out there giving them the information they need.

Gina Jurva: And in terms of the military consumers, were the numbers also pretty consistent with the public in general in terms of the types of fraud? So, identity theft being pretty high on the types of fraud that were being perpetuated against military families and veterans and others.

Daniel Kaufman: So, the types of frauds are definitely very similar. You've got impostor scams, online shopping and identity theft. And notably, I think it's about 24% of the reports we received from the military were associated with money loss, so again, we're getting a lot of reports from the military where they didn't lose any money, but 24% they did lose money. So again, we want both forms of reports, but the numbers are really quite interesting.

Gina Jurva: Well, in closing, you know what advice do you offer consumers about protecting themselves against some of these rising fraud trends, and I know the types of fraud you mentioned can be quite different, whether it's a romance scam or unemployment benefits, but what would you just suggest to the public to really, really safeguard and know that they've done everything they can to protect themselves?

Daniel Kaufman: So, the starting point is scammers are really good at what they do. You know, it is their job if you want to call it a job to get your money or your information. So, they may be pretending to be from an organization you know and they also use technology in order to change the phone number that shows up on your caller ID. They will come up with lots of reasons why they need your money or your information and only you can help. So, they'll also tell you to pay in a specific way. That's a good hallmark as well to look for. They'll insist that you pay by gift card, wiring money, or by cryptocurrency, but there's sort of a few key tips that we tell consumers. First, is slow down scammers want you to rush so they get your money or information before you have time to think. Talk to someone you trust before you act. All of our research has shown that people who talk about a scam with someone they trust are less likely to fall for it. Don't give information to someone who contacts you and go to the FTC, reportfraud.ftc.gov and if you want to get alerts from the FTC, you can go to ftc.gov/consumeralerts.

Gina Jurva: Thank you Daniel, I mean really important work you're doing. I appreciate you being out there and informing the public. Putting this report out for everyone to look at and working with law enforcement. So again, Daniel Kaufman from the FTC. Thank you so much for being a part of this podcast.

Daniel Kaufman: Thank you so much, as well.

Gina Jurva: Amanda Huston, thank you very much for joining me for this conversation.

Amanda Huston: You're welcome and thanks for having me. I really appreciate the opportunity.

Gina Jurva: So, Amanda, you heard Daniel speak a little bit about the Sentinel report? You've had a long career in government, and particularly in fraud prevention and detection, and you currently work with government clients across the country to help use technology to detect, investigate, and stop fraud, waste, and abuse. You've been in - you and I've talked about this - you've been an avid reader of this report ever since its inception, so do the results of the 2020 FTC report we've been discussing, does it align with what you're seeing in the marketplace?

Amanda Huston: Yes, absolutely. It's not surprising to see that the government documents and benefits fraud was the top form of identity theft that was identified in 2020 and the number you mentioned earlier at 2920% increase. While it is shocking, it does align with the things that we are seeing and working with our government clientele. Now, in particular, in the unemployment insurance space where literally millions and millions of claims in a single state were identified as fraudulent or singular instances of over 6,000 claims sharing the same address. When you start to look at those individual instances and then think about what's happening on a national scale. Unfortunately, 2020 probably presented this perfect storm of fraud opportunity.

Gina Jurva: I think perfect way to put it, the perfect storm. Now did anything though, even though we talked about the unemployment benefits being a really large number, I mean really, really large, did anything from the report surprise you since you've been reading it for years now?

Amanda Huston: Yeah, initially two things really jumped out to me. You know, first, I looked at the top states. As you mentioned I've been following this report and as part of the government benefit fraud space for 20 years, seeing states like Kansas, Rhode Island, Washington as some of the top states that dealt with identity theft in 2020, initially it kind of was a head scratcher for me. But then the more I thought about it is, it really does align with some of the large organized criminal rings, both domestic as well as international that we've seen target programs and there have been very widely publicized instances of scams like the "Scattered Canary", that was perpetrated in states like Maryland or Washington State and Kansas, and so these types of instances happening at states that traditionally aren't at the top of the list kind of first surprised me, but after you know thinking through it I thought OK, I'm starting to see where that makes sense, and then the second thing that you know seemed to be somewhat of a surprising trend is that younger people are reporting losing money in conjunction with fraud schemes at a rate twice as often as older people, and I think myself and others traditionally think about vulnerable populations like the elderly, who might be unfamiliar with some of the schemes that Daniel mentioned earlier, you know, that are happening both with and without technology. Some are just you know, old school phone spoofing type things. And so to see the prevalence of young people being impacted, I think for me that's still somewhat surprising, and I'd be curious to see what efforts happen moving forward from an education perspective with the FTC in terms of, you know, our national efforts to highlight these types of schemes for the elderly, we now have all these young victims who we need to make aware about what's happening.

Gina Jurva: It's such an important point. You make two really important points there, or you made several, but the ones that stood out for me when you talk about "Scattered Canary", you know, we've done some work on that and they're that Nigerian fraud ring that just was a huge part of the unemployment benefits fraud happening here in the United States and they would use all their resources, their technology resources, to try to penetrate our unemployment system and use data that they had either gotten from the dark web, personal identifying information against folks and the second

thing you said too is so important. It's just how interesting is it that younger people are also falling victim? I think traditionally we often think of fraud victims as older people or those that may not be as you know, familiar, you know, maybe English as a second language. Here it's just age seems to be a big, big factor, which is a bit shocking and I'm wondering hopefully reports like this can help educate people, so they don't fall victim. A question though for you on identity theft, so it's obviously a huge challenge faced by consumers, faced by government agencies. The pandemic exacerbated that further, and the US government, as we saw passed several, massive economic relief funding bills in a very short period of time. And government benefits, I mean the benefits fraud grew so quickly. In your research I mean, is that really a direct result like the UI fraud, the unemployment fraud, direct result of this perfect storm that you talked up earlier?

Amanda Huston: Absolutely, you know, first of all, government benefit fraud grows during times of natural disaster. Or you know sort of specialized circumstances is not new. It's not a surprise. In particular, my work for a number of years in the state of Florida in benefit programs like Medicaid, in food and cash assistance, we've seen a number of natural disasters, and then you think about large scale disasters like Hurricane Katrina. These are opportunities where there's a rapid distribution of a large amount of funds typically associated with relaxed eligibility and verification efforts. You put all of that together and it's like a giant blinking target sign for these international crime rings and domestic crime rings. We have some criminal street gangs that take opportunities here as well. And even Joe Q Citizen, right, so this singular level fraud that's happening at a large scale as well. So, it isn't surprising to see to me with everything that was going on in 2020. And then what I would say is some things that have been happening prior to 2020 that set the table for this to really create that super, you know, storm or perfect storm of opportunity. You know the first thing is technology and you know criminals have really been improving their techniques, leveraging sophisticated technology. Sometimes we think of identity theft as this crime of opportunity, you know, they steal your purse, things like that. That's not what we're dealing with here. We're talking about bots. IP spoofing, email tweaking, creating synthetic ID entities, stolen identities. Think about the amount of data breaches and really large data breaches we've seen in the last five years. Many of those identities have been breached and exposed, but weren't used, so in 2020 I read a stat that a 155 million exposed identities. Think about that's just 2020 alone. I think we all should be operating on the assumption that someplace somewhere our data got breached and, you know, it's definitely something you should routinely be checking for. So, we have our criminals improving their techniques using technology. Conversely, we've got data breaches happening, and PII or personal identifying information being released at a scale we've never seen before, and then boom! 2020 February COVID hits and now states are having to process 10 to 15 times the number of government benefit claims for you know, services and support than just the month before.

Gina Jurva: And with no warning.

Amanda Huston: And no preparation, so you know honestly it really was that perfect storm that had been building and building and building. And by the time COVID hit it, it created that opportunity for these guys to really hide in plain sight.

Gina Jurva: And you and I have talked about technology solutions in the past quite a bit, and you know, based on the scenario you just mentioned, the limited staff the data breaches, the international crime rings and it seems like technology really is one of the most important, like force multipliers against bad actors. So, just based on the work you're doing, what are some of the ways that government agencies

can improve their fraud prevention efforts, especially with those, like we said, limited resources and staffing?

Amanda Huston: Sure, sure, so let me just start by saying that kind of given all those factors that we just discussed, I'm not sure how much government agencies could really have done to prevent the large scale fraud that we saw in 2020. They were really outgunned by these criminal networks. In my career in law enforcement, we used to say that's like bringing a knife to a gunfight. You're just not going to win there and frankly over the last decade or so, as unemployment rates were at, you know, all-time lows there wasn't really a sense of urgency in investing to modernize unemployment insurance technology and systems. So now, here we are, right? And we've got these really antiquated systems in most cases that are trying to combat criminals who've been perfecting their art over the years. So, the first, you know, suggestion I would state is that we've really got to take advantage of a couple of different technology opportunities that may be out there and you know, in a more timely way, help our government agencies to become more sophisticated from a technological perspective. So, for example, scoring algorithms to triage. At this point with the volumes that they're dealing with. They need tools to help them triage risk. And what that means is that hey, when claims come through that are identified as low risk, which by the way are still the majority of the claims, most people tell the truth legitimately deserving of benefits, we need to be able to identify those low risk payments up front and move them through the process as quickly as possible to avoid backlogs. Then target and focus program integrity resources on the high-risk claims. For example, they might ask for additional documentation or have a secondary step of validation or authentication in the process. More sophisticated data analytics and technology opportunities that are presented by machine learning and artificial intelligence. Why do those matter, right? Because these guys are constantly evolving. The bad guys are constantly evolving for every step that a program integrity unit or state agency takes to close a fraud hole they are already inventing the next way to take advantage of the program. What artificial intelligence and machine learning helps us to do is to consistently identify new and emerging trends and keep improving our algorithms. And then the last thing I would say is that you know for program integrity in general, and I've seen this throughout my entire career It is really difficult to balance our need to process claims for benefits quickly because most people making those claims are deserving and eligible for those benefits and we don't want to hold them up and so typically the model really has been paying chase and what we mean by that is that we give the majority of the process the benefit of the doubt. And if we identify fraud or overpayments that have occurred, we then attempt to recover and collect. Organized criminal networks from Nigeria are not going to pay us back.

Gina Jurva: Not surprising there.

Amanda Huston: Not surprising we might not see a dime. So, we really need to move some of our investment in technology and services to the front end of the process. We've got to prevent more of these payments from being made in the first place.

Gina Jurva: Absolutely, and it's really exactly what you're saying at the beginning of the process to verify, identify identities quickly and, like you said, the goal of this fast and accurate disbursement of benefits because the vast majority of people are being truthful and they’re in need of the money. They're not fraudsters, but it's those that are that make it harder for everybody else. Now just in closing out, so I've got to ask you to look into your program integrity crystal ball, so to speak. It's 2022. The Consumer Sentinel Network data book has just come out for 2021. So, we're a year we're, you know, fast forward a

year, but what do you expect to see as it relates to fraud? I mean, are the results going to be in terms of the fraud reporting that that that Daniel talked about earlier? Is it going to be worse than 2020? Do you think it's going to level off? Like what's your prediction if you will?

Amanda Huston: Unfortunately, I think the results are going to be as least as bad as 2020. And hopefully not, but they could be even worse. And that's sobering to say for a program integrity professional, but you know it's only April and we have already seen a number of shifts and adjustments in the ways in which fraud is happening in these programs. So, as states are putting more solutions in place to prevent fraud at the front door, well, what are we doing, right? We are looking at more fraud and increasing sophistication of the fraud that we're seeing in accounts that already exist. So, for example, seeing account takeovers of people's benefit accounts such that their debit card, where their benefits might be administered to or their bank account is being taken over by the criminals. So, I think that, you know, the continued flow of funding for pandemic related assistance, continues to be a very, very attractive target, the fraudsters are adjusting, and we are already seeing that. And we've also started to see dramatic increases in other COVID-related fraud outside of unemployment insurance. So, as UI is sort of had all this national attention and focus and there's been funding and a lot of efforts by the States to get solutions in place for 2021, we're seeing increases in programs like Medicaid, the Paycheck Protection Plan, or the PPP, and in programs like food and cash assistance like SNAP and TANF, I think these programs are going to have a really tough year. As I'm not sure the level of emphasis was placed to shore up their defense systems like we had with unemployment insurance in the latter part of 2020.

Gina Jurva: And It doesn't surprise me that we're going to continue to see fraud, but we know that the government agencies are out there fighting the good fight and they have great partners like you to help them along the way. So, Amanda Houston, thank you so much. It's really always a pleasure to chat with you and talk fraud with you and hopefully we'll come back next year and do it again when the consumer sensible Network data book comes out. So, thank you so much, Amanda, I really appreciate your time.

Amanda Huston: You're welcome, thank you for having me.

Outro: 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 subscribe to this podcast on your favorite podcast platform or follow us on Twitter @TRIExecutives and LinkedIn under the Thomson Reuters Institute. Thomson Reuters Market Insights is a production of Thomson Reuters.