

TRANSCRIPT OF PODCAST

WORK WITH PURPOSE EPISODE #41

Julie Read, Director and Chief Executive, Serious Fraud Office, New Zealand

Mark Cheeseman OBE, Director, UK Government Counter Fraud Function

Andrew Walter, First Assistant Secretary, Integrity and Security Division,
Attorney-General's Department

Hosted by DAVID PEMBROKE, Founder and Chief Executive Officer, contentgroup

21 June 2021

Enquiries should be directed to Caroline Walsh on 0413 139 427 or at caroline.walsh@act.ipaa.org.au

Delivered in a partnership between IPAA ACT and contentgroup

contentgroup

- DAVID PEMBROKE: Hello everyone. And welcome, once again, to Work with Purpose, a podcast about the Australian Public Service. My name's David Pembroke. Thanks for joining me.
- DAVID PEMBROKE: I begin today's podcast by acknowledging the Traditional Custodians of the land on which we meet today, the Ngunnawal people, and pay my respects to their Elders past, present, and emerging, and acknowledge the ongoing contribution they make to the life of this city and region.
- DAVID PEMBROKE: STUDIO-19 is once again, coming to you from IPAA ACT's headquarters in Canberra, where today we are talking fraud. COVID-19 has created boom time for criminals who would seek to deceive us for financial and personal gain. These scammers and fraudsters, who've been out in force, leveraging the insecurities created by COVID-19 and the power of digital technology to launch millions of websites, email, investment employee, supply chain, and charity scams. The global reach of this digital criminal activity has forced governments, businesses, academia, and the third sector to work together, not only here in Australia, but around the world.
- DAVID PEMBROKE: Joining me to discuss this critically important work is Andrew Walter, first assistant secretary of the Integrity and Security Division at the Attorney General's Department here in Canberra. Andrew is responsible for the Commonwealth Fraud Prevention Centre, which after launching as a two year pilot program in June, 2019, has now been extended, which I'm pleased to say is bad news for criminals.
- DAVID PEMBROKE: Julie Read is from the New Zealand Serious Fraud Office. Julie was appointed as the chief executive and director of the New Zealand Serious Fraud Office in October, 2013.
- DAVID PEMBROKE: And finally, Mark Cheeseman, Director of Fraud, Debt and Grants and Government Counter Fraud Function at the UK Cabinet Office. Indeed, in 2019, Mark actually came to Canberra to assist the Attorney General's Department to set up the Commonwealth Fraud Prevention Centre. And he continues to this day to advise the centre.
- DAVID PEMBROKE: Welcome, one and all, to Work with Purpose. Andrew, if I might start with you, and I think everyone can see and feel the change in the numbers of scams. It's no longer the odd prince looking to retrieve a lost fortune, but all of our inboxes are flooded with notices to delete, to not open and to generally avoid this toxic correspondence. It's a big question, but what is government doing to effectively stem the tide?
- ANDREW WALTER: Thank you, David. And it's a pleasure to be here with you and with Julie and Mark, of course.

ANDREW WALTER: So there's a whole lot of things that are going on around government, and it depends on where you're looking, but obviously the ACCC have a really critical role that they have in relation to helping deal with scams that so many of us experienced in our day-to-day lives. And obviously we've got bodies like the Australian Federal Police and the Australian Criminal Intelligence Commission, looking at the high end of organised crime and how they are trying to lock into various programs and also go after the private sector.

ANDREW WALTER: What we're doing in the Commonwealth Fraud Prevention Centre is essentially, we're trying to harden government policies and programs against fraud in the first place, to prevent it occurring. And while we're focused on fraud against the government, it has flow on effects, because of course, fraudsters are using things like identity theft and impersonating the government officials, but also pretending to have qualifications that they don't have, which impacts on people in their day-to-day lives, and indeed, can devastate their lives if they come across these kinds of people.

ANDREW WALTER: So our focus is very much on that prevention angle.

DAVID PEMBROKE: But then in terms of building that capability, hardening that defence, what's taking place? Is it major education programs? Is it improvements in ICT systems? Just what is it that's helping the government to be more effective in managing fraud?

ANDREW WALTER: Yeah, so we're focused on a number of things. So the first is pretty straightforward, which is actually building the understanding of what the fraud problem is in government and talking with government agencies and entities about that. So for example, we know that a little under 15% of Commonwealth entities have a dedicated fraud control officer. That's less than 15% of government entities have a dedicated fraud control officer. So working with entities that don't, to build their understanding of what the benefits of having somebody focused on fraud is.

ANDREW WALTER: Also, only a third of Commonwealth government entities report any identification of fraud. So they're not actually finding any fraud. And you might say that's a good thing. We say, "Actually, that's not a good thing. It's highly likely that the fraud is there. You're just not seeing it."

ANDREW WALTER: So there's a whole range of things we're doing. One is that basic awareness. Fraud is bound to be in your system somewhere. You're just not seeing it. So how can we help you see it, and how can we help you dedicate some more resources to that? Then it's building the capacity to respond. So what we're all about is, what controls are you putting in place to stop fraudsters getting into your system? And we have a whole range of tools available, and I can send you all to our counterfraud.gov.au website, where you get a bit of flavour of that.

ANDREW WALTER: Just to give you a really simple example, we've developed a whole range of fraud personas. So we've identified the common type of fraudsters and what they get up to, and that gives you the opportunity to think about, "Oh, okay, well, if I'm a deceiver, how am I going to work my way through our systems to be able to defraud us?"

ANDREW WALTER: And so thinking a little bit more like a fraudster to try and identify weaknesses in your own systems, and then we'll work with you very practically, to try and break your systems and to try and identify where your weaknesses are. And at a more basic level, we'll also help you tell the story to your senior managers, or to your minister about why countering fraud's really important. And we've done a whole lot of work, which I can talk about some further about the human cost of fraud. For example, we've worked really closely with our international partners on that. Because it's not just about money, it's about a whole lot of other things as well.

DAVID PEMBROKE: Bet it is. So Julie, this is a global problem. So what is the experience in New Zealand, and what are you doing there in New Zealand to counter fraud?

JULIE READ: That's a very good question, David. The role of the Serious Fraud Office is very similar to that of the Serious Fraud Office in the UK, but on a somewhat smaller scale. And so for 30 years, we've been responsible for investigating and prosecuting major fraud and corruption. And two years ago, or no, three years ago now, in 2018, I had the opportunity to go to the UK to see the work of the counter fraud people in the Cabinet Office there. And I have to admit, it was a bit of an epiphany for me. I'd always talked about having a fence at the top of the cliff and not just relying on an ambulance at the bottom, in the form of prosecution, but I just was blown away actually, by the comprehensive approach that they have taken to creating a prevention function, a function that looks at the skills of individuals to counter fraud, all the things that Andrew was just talking about, all the systems that they have in place, the willingness to find fraud.

JULIE READ: So that was a really great opportunity for me. And when I came back to New Zealand after that, I certainly took the opportunity to start talking to my minister about that, in order to try and expand the opportunities for us to counter fraud in New Zealand. And ultimately, COVID really helped us with that, because of course everyone's realising that there's enormous risk to the public budget in fraud. And it affects primarily those who are most vulnerable, those who rely on government services. So that's a COVID thing as well.

JULIE READ: So we've got a bit of impetus going here under the Serious Fraud Office. But again, as Andrew said, we're looking to work with other agencies to improve their skills, to improve their capacities and to promote the counter fraud message within those agencies and the government.

DAVID PEMBROKE: So what are the one or two priorities that you have at the moment, those key areas that you're working on, that you think is going to create the biggest impact for you?

JULIE READ: Well, we're only about six months into our journey, so we're certainly the least developed of the three countries represented here today. To be honest, one of the major things that we're working on is getting that ministerial and cabinet support. So we're looking to ensure that they understand the value of this work, that they understand that finding fraud is a good thing. One of the things that happened in New Zealand a few years ago was fraudster called Joanne Harrison, who has now made her way back to the UK. And she visited Australia too, which is... Defrauded people and public money in all three countries. She's a particularly clever fraudster. She was a very senior employee in a department in New Zealand and she was considered to be really good at her job. That is until it was discovered that she'd defrauded hundreds of thousands of dollars from that department.

JULIE READ: But why I'm telling you this story is because one of the most unfortunate things that happened in all of that was that the chief executive was blamed. The chief executive was blamed, in theory, for finding the fraud too late, but this woman is really skilled and she has done this again and again and again. And so a lot of other chief executives in New Zealand said to me at the time, "There but for the grace of God, go I," and that chief executive had just been made our auditor general. He lost his job in effect, was forced to resign. And that's the complete opposite of what we want. No one wants to find fraud now. Why would they? So we've got a very big change of culture to undertake here, but I'm confident that with ministerial support and the support within the departments that we're already seeing, and in particular, our treasury, that we can make a good inroad on that.

DAVID PEMBROKE: Mark Cheeseman, conversations around risk are certainly one way to get the attention of senior executives. Was that the pathway that you took to gain the attention of the leaders in the UK when you started on this journey? And a second question to you is, through COVID, obviously COVID has had serious impacts in the UK community. Lockdowns for extended periods of time. How indeed has that changed the profile of fraud in the UK, and as the most advanced sort of counter fraud organisation in government around the world, what changes have you needed to make to stay ahead of the game?

MARK CHEESEMAN: Absolutely. So in terms of your first question, did we attack it through risk? It's an interesting one because no, we didn't, is the answer. But if I was to talk about where we are now, a lot of what we talk about is the risk management element of it. Where we really came at it from, and you talk about the leaders, and getting the leaders engaged, actually it was a lot of the leaders in the public sector who were driving this and saying, "Actually, there's something not quite right here, and we can't put our finger on it. So please can we look into it?"

MARK CHEESEMAN: So the way we really drove that change, and Andrew's already mentioned this, is build the evidence base. And the fundamental for fraud is that it's a hidden crime. People who are good at fraud hide their crime well. It is not easy to find. It does not automatically surface.

MARK CHEESEMAN: So actually where we came from it from was really understanding that nature of fraud and then building the evidence base to show what might not be being dealt with and proposing a theory that there might be a lot of fraud in there looking at comparatives in the US, in the EU, in the private sector, in academia, and looked at that to consider, "Right, what should we do?"

MARK CHEESEMAN: And that was really engaging for the public sector because they could see the size of what could be happening. And we've got to remember that fraud... Often we'll come down and we'll talk about fraud and economic crime, and we'll talk numbers. We'll talk that financial impact of fraud and the cost on public services, but some of the work the Australian centre's done is really great in looking broader at that, the human impact of fraud against the public sector, all the different impacts it has, and actually all those things which deter from what we as public servants are here to do, which is to help the government build better communities and better public services.

MARK CHEESEMAN: So our approach was really on that building the evidence base, showing over time that there was fraud out there that wasn't being dealt with. And then, very interesting, building what Julie's just said about the chief executive experience in New Zealand, actually setting a tone that finding fraud was a good thing. And that actually fraud... Trying to change this perception, that fraud is a failure into something that actually, fraud is something that happens, and it's part of being a good business, a good public servant that you look for it and uncover it. And just because you've had fraud against your organisation, does not automatically mean your organisation is bad. If you're spending millions of dollars or pounds or billions of dollars or pounds, fraud is going to happen somewhere in that system.

MARK CHEESEMAN: So trying to drive out the detection of fraud, that's really where we started. And that's what got attention, because we've increased the detection of fraud within our system by 243% since we started on that journey. And that's led to financial savings for the public sector. And it's led to more public servants and external people being found committing fraud who have been stopped. And so that impact is really positive.

MARK CHEESEMAN: Your second question was on C19 and how that's changed the profile of fraud risk. Well, the structures that we've built in the UK have enabled us to have a reasonable understanding of that, I would say. And reasonable, I'd really emphasise, is the word. I wouldn't say, "Yes, it's a good understanding."

MARK CHEESEMAN: I would say we can talk about it. And the underpinning of that, as well... And I sound like a very dyed in the wool civil servant here, going on and on about evidence all the time. But the underpinning of that was the evidence base. Because we had spent some time doing measurement exercises across the public sector, looking at comparatives, we could quite quickly draw out what level we expected the fraud to be in the system, but that's an expectation. There's assumptions built in there.

MARK CHEESEMAN: So our feel is that that's increased fraud against the public sector by billions of pounds, four to 16 billion pounds across all our schemes, furlough, eat out to help out, we have bounce back loans for businesses as well. The other impact it had on the public sector, which you'd expect, but almost as you experience it, you're like, "Aha, okay," is that it took a lot of the fraud resources off countering fraud and prevention into the frontline, into getting benefits, claimed paid quickly, getting support to communities paid quickly. So those communities could be supported and those businesses could be supported. So what that's done is it's increased the stock of fraud in the system. There's a lot more fraud in there, but it's also increased the public sector's desire to do something about it, and recognition of it. So I would say that that's probably the way that has changed the landscape.

DAVID PEMBROKE: Just in terms of that conversation around fraud. In a democratic system, which is adversarial, I can really see the challenge there around fraud, because any fraud uncovered is going to be positioned by some as a failure, as we've just discussed, that it's going to be seen as a failure. And therefore, as Julie noted that there's a disincentive for people to move after it. So how, aside from this evidence based, how have you tried to control your storytelling around fraud, such that it loses that stigma of failure?

MARK CHEESEMAN: Well, I think there's a thing here about being brave and being confident, right? And because fraud is increasingly a complex crime, and economic crime is increasingly complex. You really need experts to deal with it, certainly at the top end. This isn't something you can just look at. And actually having the experts explain the situation and be behind part of that narrative, I think is an important part. So whatever issue you're dealing with in the public sector, and this isn't true about lots of issues, but it's a generalisation, but in many issues that adversarial nature of government is going to lead to other people picking up the data points and arguing the other point of view. And absolutely with fraud, there's that potential there that someone could say, "Well, you're finding more fraud. That's because you're getting worse at dealing with it."

MARK CHEESEMAN: What we encourage, and what we help with, is for government to be on the front foot, to say, "No, this is how fraud works. And this is all built off academia, other countries' experience, there's a strong evidence base behind that."

MARK CHEESEMAN: But I was really nervous when we released our first report and our first report said, "The government is not finding as much fraud as it thinks it should. We are trying to find more fraud. And we are."

MARK CHEESEMAN: I was really nervous that all would get picked up would be the increase in fraud levels in government. But that wasn't what happened, actually. It's been quite strongly supported. And interestingly for us, supported across the systems, so supported by our parliament as well, and the committees in our parliament that hold us to account have really been very supportive of the progress. So it takes a bit of thinking about how you frame it, but I think... I'll go back to where I started. This is the part of being a public servant and working in public service is tackling these difficult issues, and putting it out there and accepting that there will be multiple viewpoints on it. And you've just got to be confident in the evidence that you have.

DAVID PEMBROKE: Andrew, it's interesting we're having this conversation, that Julie from New Zealand, Mark from the UK, there's really a heavy transnational sort of flavour to a lot of this sort of fraud, digital malfeasance. How hard is it to work across borders when you're trying to deal with some of this fraud, or counter some of this fraud, and how hard is it to work with, or how easy is it to work with your counterparts overseas to identify some of the root causes?

ANDREW WALTER: So I think that where we've got to, particularly with those members of the International Public Sector Fraud Forum, so obviously the UK, New Zealand, Canada, and the United States. So I think Mark and his team have done a fantastic job of building that as a network of support. And of course, sitting behind that is also a whole lot of law enforcement networks, which are particularly strong across those five countries as well. As well as others, including for example, the Netherlands and places like that. And there's a whole lot of other networks, et cetera, around that as well. For example, in relation tax fraud and things like that, similar networks exist internationally. So there's a lot of those connections there. I think that what's been kind of fun, as well as useful in that process has been, we're kind of all growing up together.

ANDREW WALTER: So the UK kind of got there a little bit before us, very generously have hosted us on a number of occasions. I spent a couple of days with Mark and his team before we'd even got the pilot up and running, looking at what they did, what would translate. I'd spend a couple of days in the Netherlands with their people as well, seeing what they do and what would translate there. So there's a lot of, for all of us, there's benefit in us understanding what each other is doing. What's good, what we can learn from, what we can share. There's a lot of benefit in that. And I think that network works really well. We have regular catch-ups. It's every month, pretty much. Talking about what we're seeing, what's new and in the COVID context, the UK and the US in particular, we're seeing things a good period of time ahead of us because of their different journey.

ANDREW WALTER: And so you mentioned earlier technology in your introduction, the use of SMS. Scams very early on, "Here's how you get ahead in the vaccine queue," all that type of thing. We were hearing that from the UK before it was an issue here. We're able to work in our case with the ACCC, and with the ATO and others to say, "Well, let's put out some guidance on that. How to can government agencies get ahead of that a little bit?"

ANDREW WALTER: So picking up those kind of valuable tactical lessons, as well as that more systemic lessons about how we would set this up, and quite literally we shared our pilot proposals with both New Zealand and the UK, who came back and gave us a whole lot of feedback on how we could craft it better.

ANDREW WALTER: And that's what we put to government. It was almost like a unified package of what our various jurisdictions thought a good model might be, based on their experience. So I think it's been really... I mean, nothing, here's perfect, but it's been really seamless. And just the other thing I would add is we work on common projects. So we've mentioned the human cost of fraud project. Well, everyone's inputted into that. Everyone's given our perspectives. It becomes a kind of unified product that we share within our jurisdictions. And there's a whole lot of projects that we do in that kind of space, where we all need to know more. And the evidence base, as Mark keeps talking about, is so critical. So we've got a lot of sharing going on there as well.

DAVID PEMBROKE: Julie, look, we really are only in the first innings of digital transformation, with really the impacts of artificial intelligence, 5G sensors, machine learning, cloud, augmented reality, virtual reality. Really it hasn't kicked in yet. It's coming and we all know it's coming. Is your sense of it that the threats are overwhelming, that are coming? And this sense of teamwork is going to be absolutely vital if indeed governments are going to keep citizens safe from the detection and countering of fraud.

JULIE READ: Yeah, I think it's fair to say that large sums of money have always, and will continue to be attractive to people who don't want to earn them. And so, as time goes on, they just use whatever new tools are available to them. And as you've just said, artificial intelligence, all of those things, the internet in particular has made a huge difference. And just the porousness of borders these days has made an enormous difference to the nature of financial crime, because it's certainly cross border fraud is so common now. And that's one of the really good things about having this network, is understanding how each other's systems work, lending a hand to each other. As Andrew said, that advanced intelligence that we got from the UK and the US about various frauds is really invaluable to the likes of us. One of the really good things that the IPSFF has done is to facilitate the communication between the experts from various areas.

JULIE READ: So people from our Ministry of Health got to speak with people from the Ministry of Health in the UK to talk about what they've seen. So it can be very specific. I think it's also fair to say that law enforcement keeps up fairly well with things like artificial intelligence and I hope, and I'm beginning to see this now, I'm hoping that in the longer run, as we pick up speed and a bit more expertise, that we will have something more to offer from that very law enforcement perspective. In particular, we already use artificial intelligence and a whole lot of digital stuff in our investigations, or we'd never get through them. So I'm hoping that eventually there'll be some crossover there that will be a contribution that the Serious Fraud Office can make specifically to the conversation between the three of us. But it's so important.

DAVID PEMBROKE: Yeah. Mark, it's interesting, isn't it, in the answers that both Andrew and Julie have just given, you have this sort of feeling almost of acceleration, of pace, of speed. I imagine that that would play into the hands of fraudsters. And then that's what they're looking for is chaos and movements, such that they're in a position to be able to exploit that. Would that be a fair observation, and indeed, how does government move faster, adapt quicker, to be able to be more effective?

MARK CHEESEMAN: Yeah, it's interesting, isn't it? So I just want to touch on the last question a little bit first, which is those tools and the change digitally, and how that affects both how we fight fraud, but also the nature of what we fight. And I think AI is a prime example on that because all of our countries will be thinking about, "How do we use artificial intelligence to make our control systems better, to reduce the chance of fraud, to make how we respond to fraud and economic crime better with AI?"

MARK CHEESEMAN: But we also recognise that on the other side of that, criminals will be looking at how they use AI to attack the system better. And actually, it's a bit simpler on their side, because if you're using AI to just run against the system and learn where the weaknesses are, that is a bit more of a simple task than trying to develop AI to pick up when people will successfully attack. You don't have to be a genius to work out that for the latter, you have to have some successful attacks to pick up on trends, to then to get the AI working.

MARK CHEESEMAN: Whereas for the former, you can just set it off running, and if it doesn't do anything, then you've not lost very much at all. So how that is changing, and how that dynamic of digital... We're talking about all these acceleration pieces, but how digital, and the cyber threat, and how that is expanding, and dealing with economic crime, and just changing the nature of the threat. You say acceleration and chaos and movement. It's just we're in a big change period.

MARK CHEESEMAN: And we talked about COVID-19 before. In such an international challenge as COVID-19, all of the five eyes recognised that the threat from fraud rose. Partly because public bodies had to spend money more quickly. And as a result, that meant that the controls would not be what they would be in other periods. Partly because obviously people were aware of that. You don't have to watch the news very long at all, to realise that the public sector is putting money out quite quickly. And if you're a criminal, that might be a place to focus. But also partially because we're all going to experience economic times which are different to those which preceded the pandemic, and actually in those more difficult economic times, pressures and motivators to commit fraud rise.

MARK CHEESEMAN: So actually our threat overall is going to change. Now, your question is, how does the public sector be agile? How does it respond to this quickly changing environment? And these quickly changing threats? Different departments, different public bodies can learn from other public bodies. I remember very starkly when I started as a head of fraud in our legal aid agency over here, my first step was... Right, so I wasn't a fraud expert by background. I was an ops and projects person who came into look after a fraud unit. And my first step was, "Right, how'd you do this well?"

MARK CHEESEMAN: And the way of finding that out was to go and talk to loads of different organisations and then try and work out which one of them knew what they were talking about and which one of them might not know what they're talking about, but weren't quite letting it on. The structures we're building give us that. So we have a functional centre here, which actually, if we set up a new organisation, so when we set up High Speed 2, or when we set up the response to Test and Trace, you can come to the centre, and the centre will direct you and give you guidance. And there are structures there to help you as well. So I think that structure that actually the three countries are looking at, whether we can build in our systems, will help us to be more agile.

MARK CHEESEMAN: And the other part of my answer to how to be agile as well is you don't try massive things. The temptation is... So data, we talked about digital, and we've talked about how that will help the fraudster and how it should help us as well. Well, the answer to that is to better share data and use analytics and use AI. The temptation with that then is to do a big data warehouse, where we bring all data together, a massive project where... And we put our AI across it, and that will take years and years and years, that's from my perspective. And this is just my perspective, and I'm very happy for obviously different perspectives on this, but from my perspective, that's not the way to be agile in the system. So what we do here, is we do a number of small pilots. We do lots of little pilots and then incrementally build. We start simple and then you build and build and build, and that's the way to be agile, to succeed quickly, but also to fail quickly and to have some bits that don't work out.

DAVID PEMBROKE: Hmm. So, Mark, a final question, actually, to all three of you, but I'll go to you first. The audience for Work with Purpose is very strongly the public servants of Australia. What advice do you have for them? The good men and women of the Australian Public Service who are going to work every day, most of them all wanting to do a good job. What can they do to help harden, using Andrew's language from earlier, harden the strength and the capability, that counter fraud capability in their organisations.

MARK CHEESEMAN: So I'm going to go back to where we started, if that's okay.

DAVID PEMBROKE: Sure.

MARK CHEESEMAN: And the one thing I'd want anyone listening to this to take away is that fraud is a hidden crime. Okay? It is hidden. You have to look for it to find it. You can't expect it just to crop up on your desk. And the bit that does crop up on your desk is really the tip of the iceberg. Then just take that a step further. If we don't take that hidden crime and its hidden nature seriously, it will be a problem we don't even know about. We won't see it and it will just happen. And fraud does more than lose public money, have a human impact. It also... The level of fraud in our societies kind of sets the moral tone of our nations. If we accept all that dishonesty without any impact, allowing public money to go, it sets the tone.

MARK CHEESEMAN: It's a really interesting one, that, and our role as public servants, and that's something our ministers are very keen in, and our role in saying what the, how that plays out and how that works. But beyond that understanding, it's hidden, and if we don't take it seriously, we shouldn't know about it. Get access to experts is what... Don't think you can work this out yourselves.

MARK CHEESEMAN: In the UK public sector, we are great at just trying to tackle problems, using our smarts, using our systems to do that. More and more with a lot of issues we face across the public sector, and a lot of things we want to do and opportunities that we have across the public sector, we should be drawing on experts and their understanding of that complex area, and encouraging them to lead that change, rather than trying to work it out for ourselves. And fraud's a really interesting area for that because traditionally people like me, who was just given a fraud brief... I've got very experienced investigators in my team whose first experience in investigation was not training. It was being given investigation to do. Here you go. Here's an investigation, please now investigate fraud. So get access to experts and understand where that expertise is. So those would be probably the two messages I would give.

DAVID PEMBROKE: Fantastic. And Julie, your advice for public servants as to what role they can play, how they can be more effective in countering fraud?

JULIE READ: Yeah. Obviously I agree with a lot of what Mark has just said. We've obviously been associating for a while now. I think that the thing about public servants is that most of them are there because they want to achieve something positive for the people of their countries. And in New Zealand, we talk about a spirit of service in the Public Service. So I think I would start there and say that we recognise that everyone wants to do the very best they can. And part of doing that is to look for fraud and report it. Report something that doesn't look right when you see it. So, and that's a really good thing. I guess we're still a little bit behind where the UK and Australia are, especially when Mark talked about that interest amongst departments in the UK in finding fraud. I think we really want to send everyone the message that finding fraud is a good thing. Reporting stuff that doesn't look right is a good thing, and it's always going to be there, so there's no shame in it.

DAVID PEMBROKE: All right, Andrew, the final word to you. Your advice to your fellow Australian public servants. How would you like them to act and behave to help you really, in your mission?

ANDREW WALTER: So yes, completely agree with everything Mark and Julie have said. So perhaps what I'll say is almost a summary of it. Which is to say, firstly, you have a problem with fraud. You may not know it, but you do.

ANDREW WALTER: Secondly, that problem can fundamentally undermine everything that you're trying to achieve. And like Julie, I agree, most public servants want to make a difference in the world, as do ministers. And fraud can seriously undermine that, including resulting in cancellation of programmes, and all sorts of other really serious community harms.

ANDREW WALTER: Thirdly, when you confront that realisation that there probably is fraud, there's help available. So come and talk to us, talk to other departments who do a fantastic job in this space. And there are plenty of them that really do good work. We have a whole lot of resources on counterfraud.gov.au. Go there as a starting point, but then come have a chat with us. See what help we can give you.

DAVID PEMBROKE: Alright. Andrew Walter, Julie Read, and Mark Cheeseman. Thank you so much for joining us on Work with Purpose today to explore this very important topic of fraud, and indeed how public service organisations can prepare for the threat and the growing threat that it is there. And some wonderful advice there from three very experienced public servants, global public servants who are really looking at this problem from a very wide lens, which I think is a pretty smart way to go. So thank you to all of you for joining me this afternoon on Work with Purpose.

DAVID PEMBROKE: So thanks again to the team here at IPAA for helping us, as they always do, in getting Work with Purpose to air, and to the Australian Public Service Commission, for their ongoing support, and also to you, the audience. Thank you for coming back once again. And thank you, as the audience continues to grow, thanks for your interest. And please, just a recommendation, if you see the social media promotion, a like or share never hurts. And the gold standard of support of course is a review. So if you do have the time, a review of the podcast would be greatly appreciated. Thanks again to Andrew, Julie and Mark for coming along today. That's it for now. We'll be back at the same time in two weeks, but for the moment it's bye for now.

VOICEOVER: Work with Purpose is a production of contentgroup in partnership with the Institute of Public Administration Australia, and with the support of the Australian Public Service Commission.