dspanz. digital service providers australia new zealand

Webinar Host - Ian Gibson (DSPANZ): Okay then I think we'll make a start. Welcome everyone. I'd like to start by acknowledging the Traditional Owners of the Country throughout Australia and recognise their continuing connection to land, waters and culture. We pay our respects to their Elders past, present and emerging.

Slide change

Webinar Host - Ian Gibson (DSPANZ): And I'd also like to thank our Webinar Week sponsor SuperChoice for supporting this event.

It is a great pleasure to introduce Paul Magee from Auraya who has over 20 years of experience in speech and biometric technologies. Paul has been responsible for biometric verification projects which led to improved customer experience and business efficiencies in some of the world's most complex environments.

And I actually know a little bit about Paul's presentation today. So I'm looking forward to it cause I think it's an exciting story he has to tell. If I can just remind people that if you have questions, please use the chat facility and we'll make sure they get answered. On that note, I'll hand it over to you Paul. Thanks.

Guest Speaker - Paul Magee (Auraya Systems): Well thank you Ian and thank you everybody for your interest and attendance today. I'll just start to share my screen. See if we can't get the technology to do everything that we want it to do. Hopefully you're seeing voice biometrics identity verification and a small dip into the New Zealand experience thus far.

Give me a second to line a couple of things up at my end so that I can go through the presentation smoothly.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): Okay. Today I'd like to talk about four topics. First of all how voice biometrics helps organisations to verify identity. The second thing I'll then cover is how voice biometrics helps organisations to comply with existing and emerging regulations. Then I'll head to the main topic of the conversation which is are there any lessons to be learned that are applicable from the existence today of voice biometrics in New Zealand. And I'd like to finish with a little bit of a look over the horizon about what the future uses of voice biometrics are in the markets that are operating in.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): So the first thing I'll do is provide a bit of an overview of voice biometrics and how it helps organisations to verify the identity of individuals whether they be customers, employees or in terms of government services, the citizens that we're serving.

So voice biometrics is accurate. It's more accurate than many people understand. Humans aren't that good at recognising stranger's voices and remembering them being able to identify people from their voice patterns. But voice biometrics systems have an accuracy which can be as high as 10,000 to 1 when we're listening to somebody say something where we've recorded them enrolling their voice saying that same phrase.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): And voice biometrics sits very nicely amongst other biometrics that are finding favour with organisations today to prove identity. But there's a big difference with voice over fingerprints, face and other biometric factors.

When somebody stores their fingerprint or faceprint on their smart phone, all they're really doing is creating a print that's stored in the device. Whilst it's fantastically convenient and it has levels of security that are quite useful, it only proves that I've got my device. And if I've got my device and I've got the four or six digit PIN, then it proves that whoever had that four or six digit PIN has enrolled a faceprint or fingerprint.

Now sometimes honesty's the best cure here. My smart phone doesn't just have my fingerprint in it. It has my wife's fingerprint in it. It has my daughter's fingerprint in it. As I do on their devices because if somebody's watching Netflix through my device, then if you want to put it on pause, you've got to touch the fingerprint reader first before you can put it on pause. Or if you want to make a phone call with my device, then you've got to put your fingerprint on it to get access to the device.

So if I was to use fingerprint access to access my bank account, then my wife's fingerprint or my daughter's fingerprint would also prove that it was an authorised user using my device whether or not it really was me. So the device security is as secure as that four or six digit PIN that has stored the fingerprint or the faceprint.

Now voiceprints on the other hand are created by activating the microphone on the device, collecting an audio sample from me - the user and encrypting that audio file and posting it securely behind an organisation's firewall. So when I do a voiceprint verification, it's my audio that I've just stated is being compared to the stored voiceprint that is behind the organisation's firewall that has already been tied to my identity. It can't be someone else's. So voice truly out of ban or independent of device. It means that I can verify my identity on other devices that aren't mine. I've verified my identity anywhere there's a microphone involved.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): So what problems does voice biometrics address? Well there are still some people that think the most secure things are PINs and passwords and security questions. Thankfully, most people are now recognising that PINs and passwords and secret answers to questions are not only inconvenient, they are insecure.

Passwords are not made more safe by making them more complex and making us change them more often. Passwords are stored. Now whether they're stored on a sticky note stuck to the screen of the PC that you're using or, as we would hope, stored in some sort of secure storage on your device, passwords are only as secure as the device itself or wherever else you've stored them. And we all know that passwords are often stolen or gained via nefarious activities where millions of passwords have been compromised and sold on the dark web. So passwords are not as secure as we would have liked them to be. They are broken and they're not going to be fixed easily.

And the last point about passwords is they've become so complex, get changed so often that people have to keep going back and resetting their passwords which is usually only as secure as the device where you receive the one time passcode to reset your password. So the bad actor that is in possession of your device, getting the one time passcode sent to your device is now resetting the password to get access to services. And a password when it comes right down to it, or a PIN, only verifies that the person knows the right information or has possession of the device where it's stored and it may not be the person who is the authorised user of the account.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): So. I wanted to show a simple demonstration of how voice is now being used and if you're already using this if you're an ANZ customer or another bank customer that's already using this, apologies for stating the obvious but there is a lot of people still that just don't understand the simplicity and usability and security offered by a voice print being used to verify identity. And all I'm showing here is a typical bank app where somebody does some things to affect either changes in accounts or things like that.

So let's Jennifer here on a bank app. She wants to transfer some money from her account to somebody else.

So she presses the buttons, it does what she needs to do to ask the system to pay somebody else and hang on, she's just got $1,000 in and the identity and access management says I need a second factor authentication. It displays on the same screen a microphone icon and asks her to say this transaction code. Now this transaction code isn't the same code that she said last time or any other time. This transaction code is about that particular transaction. It can be any length you want it to be. A combination between security and risk and convenience. In this case it's an eight digit code. So she touches the microphone icon, says 2493 2493. The audio is extracted from the phone. It's sent behind the firewall of the organisation that's verifying the transaction and that audio is listened to securely and if the right transaction code gets said, yes, and more importantly was it said by the person that was authorised by biometrically matching that audio sample to a voiceprint of the person that's authorised on that account.

Not only did that transaction get allowed, or processed, conveniently, simply and easily for that person but a number of other things occurred. The first thing is the creation of a non-repudiable digital signature. We have three pieces of information here. We know what device the transaction code was sent to, we know what transaction device posted the audio, we know what transaction code was spoken and we know what voice it was spoken with. That becomes a non-repudiable digital signature that allows the bank to protect itself from self fraud or fraud where tomorrow morning this person says somebody just stole $1,000 out of my account, please refund it. The second thing that happens, not only does a non-repudiable digital signature create that level of fraud protection but it also enables the regulatory compliance people within the bank to say "that account was just activated by the same person that opened the account "x" years ago. We still worry a bit about KYC compliance and re-ground truthing it but that's not an account that we need to go through the process of re-ground truthing the KYC compliance, or the Know Your Customer, compliance because we're pretty sure it's still being operated by the same person that opened the account." Where a non biometrically matched transaction code may be being operated by somebody who has phoenixed the account or has bought the account off somebody else and is using it for nefarious purposes.

So what I'm trying to say here is the simplicity and convenience of allowing somebody to simply touch a microphone icon and say allow the transaction to occur, the level of security was a significant uplift on anything else that's being used at the moment and we've got the additional benefits of a non-repudiable digital signature and we've got the benefits of re-ground truthing the transaction was done by the person who was authorised to act on that account.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): So voice biometrics can be used on apps. Obviously can also be used in browsers and therefore it gets used in transactions which are chat or messaging or it can be used in all sorts of other channels which previously weren't able to be used for transactions that were deemed at risk transactions.

In the telephone environment where most people know voice biometrics from, the voice biometric journey starts in the IVR. We all know the IVR it's where you get to punch numbers and save things before you get to talk to an agent. One of the reasons we are, as consumers, generally frustrated with IVR journeys is we can't really get the personalised self service that we want because the ability for most organisations to verify the trusted account holder or the known account holder is in fact the person calling is because we're not biometrically verified.

So when somebody comes into an organisation that has adopted voice biometrics, we start off with a simple request at the beginning of the conversation with the IVR that says so we can verify your identity, please say your phone number. Now we didn’t actually need to say please say your phone number. We could have asked you to say all sorts of different things but most people are quite happy and quite easily recall what their phone number is and say it. We use the CLI and that piece of information to make an assumption on who you might be claiming to be and then we look up the voiceprint that’s on record and say yep, it really is Paul this time calling in, now we can offer some personalised self service. I’m most likely ringing to find out about “x” or “y” based on the rest of the customer journey the organisation knows about me and it can start to provide me with that personalised self service.

If I need to go through to a call centre agent because it’s a complex enquiry and I really want to talk to somebody about it, when I get through to the call centre agent not only does the agent have all the information about me and what the agent needs to service me, and therefore not have to ask manual verification questions, but the agent actually doesn’t need to know who I am. On a screen they might know it’s a person called Paul. They can see all my bank account details or whatever the enquiry might be about but they don’t know my name, they don’t know my address, they don’t know my date of birth and they haven’t asked me those questions and therefore my privacy is enhanced and protected. But I can be agent served conveniently and efficiently because the agent knows who I was at the beginning of the call. And importantly, whilst I continue to have the conversation with the agent, the voice biometric system can continue to monitor the call to make sure that I really am the same person on the call all the way through and therefore if a call needs to get transferred to another agent, there’s no need to go and ask for a reverification to protect your security because any agent that gets engaged in this conversation will have on their screen displayed my verification status with a green tick allowing the conversation to proceed unimpeded with the bureaucracy of having to reverify my identity every time I move from one person to the next.

So the IVR and agent call is all seamless and improved because of the voice biometric component as was the ability to verify in the app. Now, today we are often being asked by organisations can you just go to the chat or the messaging and we’ll see if we can service you there because of efficiency gains. So I’m in the app or in the chat or the messaging system and I need to talk with an agent because I’ve already verified my identity with my voice during that chat or messaging process, when I get transferred from chat or messaging to an agent in this seamless multi channel environment, I’ve already been verified and the agent can pick up the conversation without needing to go through a manual verification process.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): Now. Not everybody enrols their voice and when the system first goes in, not everybody will have enrolled their voice in the system and there’ll still be quite a few people doing manual verification.

Well what can happen at the very beginning of a voice biometric system deployment is that those organisations who have recordings of fraud attempts previously perpetuated on the organisation can enrol their known fraudsters into a blacklist or a fraudster list. And every time there’s a conversation whether it’s a conversation in the IVR, conversation with a bot or a conversation with an agent, we can send samples of that voice to the fraud detection system to work out whether or not this person who hasn’t been biometrically authenticated or biometrically verified are they somebody we know not to trust. And if they are, what action do we now take in real time to ensure that they aren’t able to do an activity that impedes on my other customers by doing an account takeover or some other fraud.

So thwarting bad actors who are trying to attempt account takeover or other bad acts can be caught in real time. And if you find somebody that you think is a bad actor, you can go back and compare their voice with previous suspicious activity and get a real time and historical analysis on fraud attempts against the organisation by specific people.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): So in summary, what I was trying to set up here is what does biometrics do, who does it do it for and what are the benefits.

It allows organisations to complete risk transactions without post-call secondary processes to authorise transactions thanks to the non-repudiable digital signature that’s contained in the metadata of any voice biometric verified conversation.

It increases organisation’s efficiency by eliminating manual verification processes and the processes such as email verification links and sending one time passcodes to get people to verify who they are. It’s not just efficiency in that. It’s actually also about customer experience and it’s also about the real level of security. Continuing to send one time passcodes or email links to the device that I’m already using doesn't actually add any security, it just allows us to say oh we tried two or three different processes to make sure we verify the right person. The fact that they have access to the device means you’ve just made the journey of a legitimate customer more difficult and you didn’t make it any more difficult for the bad actor that had access to the device.

Using voice biometric allows you to increase data privacy protection because you don’t need to expose confidential PII to anybody, you just need to verify their identity by listening in the background to their voice. It reduces fraud losses, minimises reputational damage by account takeovers, identity theft and others. And allows real-time fraud detection with fraud management systems.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): Now. How did New Zealand do this? Well the lesson from New Zealand is that …

Slide change

Guest Speaker - Paul Magee (Auraya Systems): … there's five million citizens in New Zealand. Inland Revenue and Ministry of Social Development, here in Australia we call it the Tax Office and the Centrelink office, have been using voice biometric technology for over a decade. BNZ was one of the first banks in the region, in the world, to deploy voice biometrics the way they did. And lots of other organisations, since those organisations started the process, have deployed voice biometrics.

Now, that means more than 75% of the New Zealand adult population now enrol their voice in systems to verify their identity and get access to secure, convenient service from government departments. Virtually all government departments now use voice biometrics for verifying identity. And the two biggest banks have deployed voice biometrics in customer facing applications, that is BNZ and ANZ and smaller banks now are deploying it as well.

There's an oft repeated refrain when I talk to organisations in New Zealand that have not deployed voice biometric and that is when somebody an organisation that's not using voice and they start to ask for name, address and date of birth and other personal identifiers, often the person turns around and says why are you asking me these questions? Why aren't you just using the voice thing? I don't want to tell you all that secret stuff. Or, I can't remember some of the answers to some of the questions you're asking. So voice biometrics is well over the threshold in New Zealand of being the preferred system for customers verifying their identity especially in over the phone conversations.

The penetration of the technology into these organisations and their successful uptake I think is where the real lessons can be learned for those that are now considering the deployment of voice biometric to add these benefits to their own organisation. And one of the most important things was communicating with the people that were being asked to enrol and that's one of the things I wanted to try and demonstrate here.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): Delivering messages to those that you're asking to enrol showcasing the benefits that they are going to get from participating in the process. And there's very few people today that don't have some concern about their own privacy and their own exposure to being attacked or hacked or having account takeover or having their identity stolen. So if you provide people with this message that I'm introducing some technology today to help you protect your identity, protect you from being hacked or attacked, that's the benefit to people. The second benefit, and it is secondary to this, is and it's going to be quicker, easier, faster, simpler and make it easier for you to do business with us in the channel of your choice.

So they get the safety and security benefits, then they get the convenience and speed benefits and then you make it easy for them to enrol by allowing them to enrol on their channel of choice. If they use email, if they use chat, if they use an app, then allow them to click through from those channels to enrol their voiceprint, verify their identity and from then on, use their voice in the channels that they want to do.

We also saw that customers who were approached to enrol their voiceprint when they were doing an event like opening a new account, starting as a new customer so where in the customer journey do you enrol these people became quite critical. So any time there was an opportunity to enrol a voiceprint when an event occurred in their customer journeys that meant they were willing to go through the couple of minutes required to do the enrolment and verification of their identity to associate their voiceprint with their account. So enrolling via websites and mobile apps became a big part of it and enrolling whilst changing their account status on other issues was also a big part of it.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): Now I've got here a video which should just magically appear showing one of the messages that IRD used in the early days. And you'll see how it was couched around the benefits to the customer or the citizen.
IRD Youtube video on voice ID plays

Video voiceover: Make it simpler, faster and more secure when you call Inland Revenue. In this video, we explain the benefits of Voice ID and how to enrol. Voice ID uses your unique voiceprint to quickly and securely confirm your identity. Calling us will be quicker, easier and you'll no longer need to answer questions to prove who you are. Once enrolled, you can find your IRD number, change your details like address and bank account and reset your password for myIR Secure Online Services. Enrolling is easy. All you need to do is get your IRD number. You can find this on a letter from us, your pay slip or by logging into myIR Secure Online Services. Find a quiet place and call us on 0800 257 843. And that's all there is to it. Enrol today to enjoy the speed, security and simplicity of Voice ID.

Video ends

Guest Speaker - Paul Magee (Auraya Systems): Well thanks for playing that video for me. It was going to appear automatically in my presentation when I touched a key but five minutes before the meeting started, we worked out there was a workaround to it *inaudible.* So thanks Maggie and Donna.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): So voice biometrics in New Zealand has resulted in about 75% of the New Zealand adult population having registered their voiceprint. About 90% of MSD clients are verified prior to talking to an agent. That means they've all had a chance to be personally self served in their IVR and when they've gone through to the agent, then they are who they say they are. It's an unbelievable statistic in terms of efficiency of that contact centre.

And 70% of regular callers to the BNZ use voice biometrics to verify their identity. Now lots of people call their bank once every 10 years because of an issue or they may not even be a client and they ring a bank. So there's always got to be other ways to verify people at least to establish an identity.

Recapping, 75% of the New Zealand adult population have registered their voiceprint. 90% of MSD clients are verifying prior to talking with an agent and 70% of regular callers to BNZ use voice biometrics to verify their identity. They're some of the higher level stats from a country that has had massive uptake of voice biometric.

How does that compare? We think about, and some of these are educated guesses but they are still guesses, but we think about 30% of the people in the UK have enrolled their voiceprint to verify their identity. HMRC, which again is like the Australian Tax Office. They've got some of the biggest banks over there Barclays, Lloyds and HSBC have been using voice for a number of years and there are some smaller organisations.

And here in Australia, about 35% of the Australian adult population have registered their voiceprint mostly with ATO and Centrelink but some banks as well. And telcos are now looking at expanding their use of voice biometric not only for efficiency and customer experience gains but for the security benefit of knowing that they're not swapping SIMs with the wrong people or other risk transaction.

Surprisingly for some, the voice biometrics penetration in North America, what we call USA and Canada and Mexico, is less than Australia and UK and a lot less than New Zealand. So only about 25% of North Americans have registered their voiceprint to deal with organisations there. Although, today, the growth is much faster because there's a significant uptake because voice bots and cloud based delivery of services is accelerating the take up, again, in the small SME market there. So it was the big organisations that had millions of calls that were doing the complex lifting of putting voice biometrics from the contact centres, now that's become quicker, faster and easier to deploy voice biometrics then the uptake is happening in the smaller organisations that get the benefit of cloud based size and scalability. The other thing, especially in the US, that's driving uptake of voice biometrics is in health services where not only is the efficiency and security for this much bigger demand to be able to not only provide privacy but prove that the effort has been made to make sure that only the authorised people are able to get access to health services information.

I didn’t spend a lot of time on this but often voice biometric in a regulatory compliance area is to say well we only provided the information to the authorised person and we can prove it which becomes important when hang on well how can you prove that it was the authorised person if the only evidence you’ve got is the access that they said the right knowledge based questions or provided the right password. Somebody can’t say well you didn’t give it to me. While if you’ve got their voice captured as part of the process and you can show the score and then you can show that it really was the person that was authorised that got access.

In Asia, the Middle East and Africa, they’re at a much earlier stage of adoption of voice biometric. But Africa’s an interesting market in that there, a lot of banking occurs where the phone is in fact a virtual digital wallet and so that security of the digital wallet not able to access the phone unless you are the authorised person is driving uptake of voice biometrics amongst telcos and banks providing those digital wallet type services in Africa.

Now voice biometric is growing globally. The fact that it’s more advanced in terms of market penetration in New Zealand than virtually anywhere else in the world just gives an idea of what New Zealand has done well and been able to achieve.

Slide change

Guest Speaker - Paul Magee (Auraya Systems): So. I’ll get to this future trends issue and then I think Ian we’ve got time for questions, if any, from the audience.

Government agencies and private organisations are now moving to provide a service where consumers can allow those organisations to have their voiceprint stored. And what’s the benefit of that? Well somebody’s gone to the trouble of verifying their identity, creating a voiceprint to deal with one organisation, then if they’ve got to go through that same process to deal with the next organisation or swap from one bank or telco provider to another, they’ve got to establish their identity and create their voiceprint. Whereas if one organisation, that is trusted, has access to your voiceprint and a verified status that you are certified, that that voiceprint belongs to you, then you can give any organisation that you deal with permission to reach out to that organisation, establish your credibility and then serve them comfortably and confidently. Much the same as what we do with allowing organisations to access a government service to check that my drivers licence is really issued to me allowing me to open a bank account. And so this process of allowing organisations to hold a secure voiceprint is at early stages but it will make it easier for organisations to use voice biometrics where they don’t have to get everybody to enrol first and it allows people to have secure process to deal with new organisations or different organisations.

Voice biometrics will be more widely used by security agencies. It is already being used. But there's been huge investment over the last decade or two in converting audio into text so that AI engines can search those lakes of information to determine what people are saying to pick up on terrorism events or criminal activities or other issues. Today, that's not going away. That's more and more of that. But what we can now do is offer those organisations the ability to really concentrate on the conversations where person of interest one and person of interest two are in the same conversation. And that can be done in virtual real time. So if a conversation starts between me and Ian, then somebody who's interested in what we're saying together will be able to say this is an important conversation because two persons of interest are in this conversation and so we should examine it carefully.

Using similar technology and this is at an even earlier stage but I think it's going to be a powerful additional reason to use voice biometrics, is where organisations that are already tracking movement through websites and emails and other things to determine trends and they're listening to the conversations people are having with bots and agents to determine what the hot issues are today that something is broken or something's not working or some message isn't getting through from our advertising. Understanding what people are saying provides real powerful insight but what voice biometrics can do is add to that wealth of information by determining okay the people that sound angry, that sound old, that sound like males are the ones that are mostly complaining about this issue. So we can use voice traits to add to the richness of data that we're examining and analysing and drawing conclusions from. So our voice discernable traits are quite powerful that showing people we're angry, we're sad, we're happy, we might be in a mood to buy, we might be in a mood to do all sorts of things based on our voice trait. Humans are pretty good at understanding what a voice trait sounds like and what it might mean but so is a voice biometric engine to determine that insight.

Slide change

Host - Ian Gibson (DSPANZ): That was great. We're probably a little pressed for time but there are a couple of questions I wanted to shoot your way. It seems that facial recognition, probably isn't a day where that's not in the press, and given the issues that have been raised with it, why do you think voice authentication isn't more popular than it is?

Guest Speaker - Paul Magee (Auraya Systems): That's a really good question and I wish I knew the answer. I think it's because I don't do enough of these conversations. Voice biometrics unlike face, people can take your face whether you like it or not. You can put your mask on, your sunglasses and your hat but they can still take a photo of you. If I choose not to speak, then nobody gets it. The other side of it is most of us, almost all of us, are quite happy to answer I don't want to tell you my age and I don't want to tell you all sorts of other things but I will say that yes I want to deal with you and I'll tell you my phone number because that's a public piece of information. Or, if I don't want to tell you my phone number, what numbers do you want me to say and I'll say those numbers because they mean nothing to me and I can verify my identity. So we're much more in control biometric than face.

Host - Ian Gibson (DSPANZ): And just quickly, I know both New Zealand and Australia have been going down a path with the trusted digital identity, do you think there's a place for voice as part of that framework?

Guest Speaker - Paul Magee (Auraya Systems): Absolutely and never let me say that I think voice is the only path. I think it's the most important but in the arsenal of trying to give what we all want which is convenience and security and privacy, voice adds a significant element. It's the times when I don't have the trusted device but I still want to be recognised, I can use my voice. If I've got the device and my voice, then I'm recognised easier. So device and voice and face and fingerprint and other methods are all part of the mix but I think voice is the most flexible.

Host - Ian Gibson (DSPANZ): Yeah. Fair enough. Now I know there was the intention to do a poll today. We don't really have time for that sadly. But I know Paul didn't mention this specifically for that reason but not many people probably realise the ATO have approximately 6.5 million voiceprints on their files. So it's quite a significant number.

Guest Speaker - Paul Magee (Auraya Systems): Yeah it's a great testament and shows that where it makes sense, people are using it and it's a testament to the resilience. People have tried and tried and tried. It's now got to that stage and it's working well.

Host - Ian Gibson (DSPANZ): Okay. Well perhaps on that note I'll bring it to a close. I'd like to thank everyone for their attendance. I'd also like to remind you to thank our sponsor SuperChoice who is sponsoring Webinar Week this week. I'd also like to remind you not to miss tomorrow's session which I'm sure will be another interesting session on eInvoicing at 11:00am eastern summer time. And a reminder that this session has been recorded and will be made available to attendees and on the DSPANZ website over the coming weeks. Follow up questions can be sent to hello@dspanz.org and on that note I'd like to thank our audience and Paul for a really interesting presentation today. Thanks Paul.

Guest Speaker - Paul Magee (Auraya Systems): Thank you Ian and thank you everybody else.