

PRESENTER: Joining me now is Steve Ackland, CEO of AIM, to discuss how pension scheme managers and trustees can keep member data up to date and secure, so it's good to have you with us today. STEVE ACKLAND: Pleased to be here. PRESENTER: So when it comes to member data then, what are the main challenges for 2019? STEVE ACKLAND: So, there's a lot on their agenda, a lot in their in-tray at the moment. Obviously when you start looking at things such as GMP reconciliations, understanding their liabilities; GDPR, General Data Protection Regulation, securing their data, liabilities; as well as areas such as Master Trusts and consolidation. There's an awful lot they have to worry about. The thing that brings them all together, which is where data is very important, is that data underpins all the success for each of those initiatives. And that doesn't even include their day-to-day work when it comes to doing things for example such as security and protection, making sure people get paid on time. And all those sorts of areas where again getting efficiencies out of the system, all of that is reliant on having good quality data. So therefore that is why it is a very hot topic and very important at the moment. That's been recognised not just within the industry, but also outside, and obviously government is also pressing on organisations and providers to make sure their data is as up to date and in good condition as possible. PRESENTER: Now, the pensions dashboard is poised to launch in 2019, so are pension schemes prepared for this? STEVE ACKLAND: That's a very good question, and just going back a few steps in terms of what the pension dashboard is aiming to do. It's a very noble initiative. The only thing about it is it's been around for a few years. Now the objective of the dashboard is to ensure that anybody who has a pension can actually go onto a web-based app, log in securely, and then identify what they've paid in, how much their pension is currently worth, and how much it'll be worth when they retire. So it's all very good stuff. Again, underpinning all that of course is going to be data. Two things are required for the pension dashboard to really be successful. The first one is about inclusivity, so making sure that all the stakeholders enrol and sign up to it, and the second one is around trust. If the information that they get out of it is inaccurate, not up to date, then of course that trust will be lost. So as you can see the dashboard actually is a great incentive for organisations to make sure that their data is up to date and accurate and compliant, rather than just leaving it almost to the last minute when people retire, which has happened quite a lot in the past. So how do we therefore drive the dashboard in terms of data? Well it's a great opportunity therefore for organisations, for trustees, for scheme managers to start looking at their data. Normally that probably will either involve some ongoing initiative, or some sort of project. But this now needs to be widened into a far greater analysis for what information they have, and where that is kept and held, and making sure that data therefore is kept up to date and in good shape. And there are ways and means of actually doing that, which obviously people are now looking at. PRESENTER: So then what do pension fund trustees need to do to be ready? STEVE ACKLAND: So the dashboard, as I just said, is something which is driving the ensuring data is clean and compliant. And a way of obviously looking at this, the approach that we take is five steps, is to make sure that data is in good shape, and trustees and scheme managers can therefore take the following. So step one really is about discovery. And this is something they can do urgently. Because the dashboard is targeted to come in in 2019, although some of the commentators are saying actually it might be as late as 2026 by the time it's fully up and running. But what they can do is to actually look at their scheme data, their member data, and they can do some analysis and discover really what the scope of the non-compliance is with their data: how out of date is it, how inconsistent is it? Once they understand what that is they can then go onto step two, and step two is about looking and understanding therefore the scope, the resource requirements, and perhaps the cost to actually get that data into good shape. Then they have to prioritise it. Step four is then to go and remediate it, so clean that up, make sure it's all in good shape and consistent. Because again the dashboard will be very unforgiving when it comes to inconsistent data, and you will lose that trust as I've said previously. And then finally make sure that project transitions into an ongoing process. That process is about making sure that data is consistently and continually

cleaned, make sure it's up-to-date. It's not just a one-off thing which you can then forget about for another year or two; you have to do that consistently. So they're the approaches to take, and of course to keep the costs down you have to use automation and software tools to do that. And of course there are some on the market which will allow an organisation to do that effectively. PRESENTER: So how then can pension scheme managers and trustees improve the integrity of member data? STEVE ACKLAND: So, by applying that approach, taking those five steps, and using tooling to actually go ahead and do that, they will actually understand what their risks are, what their liabilities are. For example a scheme which hasn't been properly assessed in terms of its data, valuation is therefore difficult to predict. Is it accurate, therefore have you got enough scheme funding in it? And by applying those simple five steps moving from project into ongoing process and applying tools, you will be able to get your data into good shape. Now, the issue around urgency, 2019 of course is literally just around the corner. If that is going to launch in 2019, then our feeling is that all organisations are not going to be ready. Maybe even the dashboard won't be completely ready. But if it is, then probably DWP and the government will need to implement it on a phased approach, very much like auto-enrolment. So even though organisations need to start pretty quickly, there may also be a little bit of time for them to get into good shape. But having a plan together now as to how they approach it, and understanding exactly through that discovery step how non-compliant their data is, is a very important first step which organisation scheme managers, trustees, must get done as soon as possible. PRESENTER: And can there ever be one source of truth? STEVE ACKLAND: That can mean several things. So, in terms of the provider, there should always be one source of truth. In terms of will there ever be one huge database where everybody's pension details are in, highly unlikely, I don't really see how that's ever going to happen. However from the consumer's point of view, the person who's going onto the dashboard for example, then absolutely there does need to be one source of truth. And that source of truth is what information comes out of their dashboard. So that is a very important objective, and that again underpins the trust requirements. PRESENTER: So cyber security and prevention of pension scams finally. Now these are high in the minds of pension scheme trustees and managers, so how can they make sure that they don't fall foul to these? STEVE ACKLAND: So everything's gone digital, the world's gone digital. So has crime, and obviously we call that cybercrime now. Pensions data is very personal, it's very financially orientated, so therefore it's a real target for hackers. So obviously it has to be protected. Whether a scheme is being managed internally or externally, then you follow the same sorts of rules. You first of all have to understand what the risk is, so what that data is, where it's held, what category it is, what its risk and liabilities are going to be. Understand that internally and externally. Then you work at making sure you have controls in place, because cyber security and breach is not just around some guys in hoodies sitting in coffee shops trying to hack into any of the big databases. It can be about an individual who accidentally has sent out a wrong email somewhere to the wrong person with some personal details, or personal details even getting out of an organisation. So you have to put controls in place. You have to train your staff to make sure those things don't happen. Once you have those in, then of course you need to look at the big hitting cyber security software, which will therefore protect penetration, people trying to get into your network, most importantly trying to leave with information. But an organisation should now look at what they call the third generation tools, and these are tools which not only protect in an anti-virus type of way your boundaries of your network, but actually also detect things through artificial intelligence such as zero day attacks. And these are the sorts of attacks which we hear about in the news, whereby an organisation has been attacked some months before, it only becomes detected sometime after when all the damage has been done. Three easy steps to use for an organisation: manage and learn what they're doing, and how they're doing and success. PRESENTER: Super, Steve, thank you. STEVE ACKLAND: Thank you.