PRESENTER: Well, Gillian, let's start with a catch-up really. What's been happening in the regulatory space since you were last on here? GILLIAN: So I think since I was last on here we've seen MiFID II, PSD2 and GDPR go live, come into force if you like, and also the FCA have issued their 2018/2019 business plan. PRESENTER: So, then, Michael, what sort of legal issues have arisen; what do you think people have had to deal with? MICHAEL: I think we've seen a variety of things really. We've had recent cases in relation to privilege from a legal perspective. So where financial services firms are getting advice or undertaking investigations, what they can retain and don't have to disclose to the regulators being one of the key areas. We've also seen a recent case in relation to PPI and recovery of commission, so that's still ongoing. And we've also seen various issues in relation to cybersecurity, and how firms deal with that, deal with both the FCA and the Information Commissioner's Office as well. PRESENTER: So, Michael, any legal issues that have arisen and things people have had to deal with? MICHAEL: Yes sure. We've seen a variety of things I think over the last few months; one being privilege. There's been quite a few cases and a bit of focus around how firms deal with them getting advice, what they do with that advice, how they can retain that advice, and not necessarily pass it on to the regulator and protect themselves. We've also seen a recent decision in relation to PPI and recovery of commission. We've also seen some focus on cybersecurity with firms, and how they interact with the Information Commissioner's Office, and also the FCA at the same time. PRESENTER: So we're going to dig into those issues a little bit later on. But Gillian, in terms of sentiment, how have people reacted to all these different changes, what have you seen? GILLIAN: So I think firms are trying really hard, I really do, and they're trying their best, but after for example MiFID II came into play this year had issues themselves. So I think very much firms are now focusing on post go live and ironing out any issues that remain within their own firms. PRESENTER: So people are still very much finding their feet when it comes to this regulation. GILLIAN: Yes, I think they are. PRESENTER: So then we've recently had the FCA business plan. So what do people need to know when it comes to that? GILLIAN: Well I think in terms of the key focus Brexit does take centre stage, but there's also other priorities within the business plan, and really that's a continuation of the work that the FCA has already started. PRESENTER: So the FCA has highlighted seven cross-sector priorities for the coming year, so talk me through those. GILLIAN: So the seven are, first of all there's culture and governance of firms. We're seeing that a lot. That's being discussed a lot within the financial services industry, and certainly with the Senior Managers and Certification Regime coming along. Again that should take centre stage and go hand-in-hand with that. There's very much innovation. So the likes of tech innovation, big data, there's data protection, resilience and outsourcing. But also other things like how you treat your customers, particularly existing customers. There's also high cost of credit. They're also looking at longer-term savings, so pensions, and also the generational differences. What younger, older people, what savings and longer-term savings mean to them. There's also tackling anti-money laundering and financial crime. And I think I've covered them all there, yes I have. So yes it's that continuation of themes that we've already seen from the FCA. PRESENTER: So any perhaps issues that could arise out of those Michael that you see any traps people could fall into? MICHAEL: I think we've seen a continuous approach from the FCA. I don't think it's overly surprising that they're still the themes. I think they seem to have carried on, they're early. But I think in terms of traps, we've had quite a number of queries in relation to anti-money laundering, and when certain regulations may or may not apply, and who's caught by those regulations, and what they need to do if they are caught by them. And as I said earlier on in relation to cyber, there's been quite a focus within the regulatory community on cybersecurity. How to deal with that, what are their systems and controls? Do they really even understand where their data is? I mean we've had various instances where we're speaking to client, and the first question we'll ask is well where's the data that we're talking about, and sometimes they don't know. Sometimes it's held in a cloud, and nobody really understands where the cloud is. So you're going to see, or you are seeing the

FCA ask a lot of questions around that. Which firms were getting to grips with, which they haven't necessarily done in the past. PRESENTER: And considering that, is there a checklist you think firms should be doing, tick-off points that they should make sure are there? MICHAEL: Yes, I mean the FCA doesn't like tick lists as we all know. It's not a tick list compliance culture they say, but yeah I mean there are certain key things that clients can do, and certain key things that firms and individuals can do in terms of their understanding. For example if we focus on data, what data they hold, why they hold it, do they still need to hold it, is it still reasonably to hold it, where's it held, is it secure, who's responsible for security – there's a whole list. And there is a list that people can run through just to be able to put them in the position to answer the questions they're likely to face. PRESENTER: So the overall focus of the FCA then, Gillian, what would you say it is? GILLIAN: I think actually there's a really good quote actually within the business plan from Andrew Bailey, who's the CEO, and I'm actually going to read it out here. He says that firms' culture and governance is pivotal to building public trust and confidence in the UK's financial services industry, both domestically and internationally. We've heard that from the FCA before. So I think really to sum it up it's about good customer service, as well as embracing tech innovation to meet regulatory obligations. Because tech can allow firms to offer better services and offer better products to mitigate risk, to increase competition, as well as being able to truly protect client assets. PRESENTER: Well earlier you mentioned changes to SMCR, what are we looking at exactly there? GILLIAN: So with the Senior Managers and Certification Regime the FCA have recently published near final, they're not quite final but near final rules in terms of implementation of the SMCR for solo-regulated firms. And that specifically means for firms that are regulated by just the FCA themselves. Now very little has changed since the consultation paper, and 272 firms actually did respond to the consultation paper. But I think it's worth nothing one of the small changes if you like, is it's much easier to opt to be an enhanced firm. So you come under more scrutiny under the SMCR if you like. So an enhanced firm is your much larger firms. So for example a CAS large firm would be an enhanced firm under the Senior Managers and Certification Regime. But coupled with that the FCA also want to, or are proposing having a directory of individuals who work within financial services. Now what that means is it's really about verification, so a consumer or firm can verify who that individual is, whether they be a senior manager, an approved person, or indeed someone who's in a customer facing role that requires qualifications. PRESENTER: And the importance of compliance, Michael, when it comes to this, what are we looking at? MICHAEL: Yes, it's really key. I mean the directory is an interesting one for me, in the sense of the directory is going to contain a register of everybody who's both a senior manager, but also certified by the firms. And the firms who are certifying those individuals, the FCA doesn't really have a lot of oversight of that. So there are going to be individuals on the directory that the FCA don't really know, haven't really met, haven't really scrutinised, and they're therefore relying upon the firms themselves to conduct that assessment. The key question then comes well what if the firm gets it wrong, and somebody's on the directory and they're not necessarily appropriate to be certified. But customers and retail individuals can look at the directory and say actually they're on the directory, why shouldn't I use them? And how much trust and reliance can be placed on that directory as a result I think is still a question to be answered. I think in terms of as you say in terms of compliance by firms in general, it's pretty much a consistent approach from the FCA. I think culture is clearly a key issue. Senior management responsibility as you said is a key thing. The FCA, and the PRA in many ways, are desperate to hold individuals accountable, and that's why we've seen this year already a number of final notices and penalties imposed on individuals by the FCA, which not necessarily the kind of high profile individuals they've been seeking, but there are an increasing number. PRESENTER: So then in terms of FCA enforcement, what sort of action have we been seeing? Give me some examples. MICHAEL: Sure, we've seen a few in relation to firms already this year, and the most recent was Canara Bank, so a focus on anti-money laundering, their systems and controls. It's part of an ongoing theme we've seen in the

business plan this year, we've seen in the business plan last year, the FCA's focus on financial crime, and also preventing money laundering. To the extent they've even said they're going to use their criminal powers for the first time to prosecute firms and/or individuals who fail to conduct themselves properly in that space. That was an interesting point in the business plan, on the basis that I think when it was first flagged in the business plan, I'm not sure the FCA knew they even had the power to prosecute criminally. I think there were lots of people running off to find books and find out how they'd do it. But they've said that's what they're going to do, so I think we almost have to expect that that's going to happen. PRESENTER: Do you know what sort of penalties we're looking at? MICHAEL: I mean currently financial penalties, so penalties in terms of hundreds of thousands, all the way through to hundreds of millions in the case of Deutsche, which was last year. We're also seeing penalties against individuals who are potentially involved as well. So you go back to Bank of Beirut's Sonali Bank, about 18 months, two years ago, individuals were also fined at that point. Firms are also getting restrictions in terms of taking on clients. So for example if they've failed to undertake appropriate due diligence they're getting restrictions on taking on new clients, and that's having quite a significant commercial impact as well. We've also seen a recent enforcement action in relation to market abuse systems and controls, so again the kind of focus around the areas of financial crime more than anything else at the moment. But we know from speaking to various people within the FCA, but also from speaking to our clients and who we're seeing on the ground, that the FCA's active in a number of areas in relation to enforcement across a range of things around product governance, advisory, client money. We're also seeing work around statements to the market, misleading statements to the market, insider dealing. So they're pretty active in a range of things, a range of areas. More recently in March the directors came out and said they want to do more enforcement cases. They don't want it to be seen as a burden or a negative thing if someone's under investigation. It should just be increasingly the norm. Not sure I agree with that, I think a lot of firms and individuals would hate to ever be under investigation, particularly individuals who lose a job as a result, or may not get another career. But that's what they're saying anyway, so [unclear 0:10:58] saying lots more investigations. We've seen from a statistic point of view I think they opened about 70-odd insider dealing investigations last year. They opened about 12 to 15 the year before, so quite a significant increase. And continued focus on criminal work, criminal prosecutions, criminal investigations. PRESENTER: So, Michael, are there any common or very avoidable mistakes people are making, and how would you suggest then that people really safeguard themselves? MICHAEL: I think some of it's around knowing your business. I think much of it is where firms or individual senior managers have focused for a period of time on certain key areas, and haven't potentially looked at the newer areas that the FCA is developing an interest in. Which is why we get questions, we get advisory work and compliance queries around things like financial crime systems and controls. Things like an anti-bribery review, things like an anti-money laundering policy, and how it's used, how it works in practice. I think for me one of the key things is senior management, and I think we've both said it already today, I think senior managers understanding how their business works, and particularly the areas that they're responsible for. And not being afraid to ask questions, not being afraid to poke and prod. Because I think historically, it's not just financial services firms but firms in general, almost don't want to know. Because the business is working well, it's commercially viable, it's commercially profitable, and it's like well I don't really want to look over there because what might I find? Whereas I think now they're having to. They've been given the responsibilities, the key areas, and now they're having to ask those questions, and if anything it will protect them in the long run, but it's just not having that fear I think. PRESENTER: Well clearly this is an incredibly complicated topic. Gillian, are you thinking it's holding people back, because they are scared to ask questions, they're just worried they're going to look incompetent maybe or they're just scared to do things because it's quite a new thing? GILLIAN: I think it goes back to the culture of organisations, some are better at it than

others. I think with the Senior Managers and Certification Regime that notion that you could be held personally liable, that's quite daunting actually. And if there was say a conduct rule breach, you could lose your job. That could end your career. I don't think it's ever been quite so forthright in terms of what could happen to a senior manager should that occur. So I think it is quite daunting. You do hear some people saying I don't want that role anymore, I don't want to do that! And I don't remember a time when perhaps people were quite as vocal. But as I say I do think it goes back to the culture of the organisation. You know, staff at all level have to understand the role of what they're doing, and understand what they're responsible for, understand that they are accountable – maybe not in the same way as a senior manager or a certified person, but they still have a role to fulfil and they have responsibility. And I think if a firm embraces that as a whole, then that will stand them in better stead for the future. PRESENTER: And then Michael how do whistleblowers fit into all of this? MICHAEL: Yes, I mean one of the key areas the FCA has said is we want whistleblowing. They've got a whistleblowing champion now within the senior managers regime. So they're looking for a focus by firms on whistleblowing. I mean the FCA historically has always receiving whistleblowing complaints to itself. What it's looking for is it's looking for those to go through the firms, through the regulated firms to be dealt with appropriately, and then to be reported as and when is appropriate to the FCA. Whether or not that's happening at this point in time is a matter to be seen. I think the larger firms and the institutional financial services firms have had whistleblowing lines for a long period of time, and they've utilised that information. I think medium to smaller-sized financial services firms, it's an interesting challenge for them. And I think it's an interesting challenge for the people who are being asked to blow the whistle as well, on the basis that they often receive negative reaction internally. They may lose their job, they may suffer some detriment. And again there was a query, a question I think that was raised in The FT the other day around what do I do on the basis of if I've blown the whistle and my career for example hasn't gone in the same direction as everybody else's, who for example started with me at the same firm, is it because of whistleblowing? How do I explain that if I ever want to move career? I mean I've known a few whistleblowers now, high profile whistleblowers, and I don't think any of them have any regretted actually blowing the whistle. But some of the reaction that they've had has been pretty extreme, to the extent they've lost jobs, they've lost homes. They've been unable to find alternative work, and this is with and without children, and it's taken a period of time for them to get back into work of some description. So it can be quite a significant thing. PRESENTER: It doesn't really sound very encouraging to be a whistleblower there. So in terms of remuneration, their rights, what are we looking at? MICHAEL: Yes, obviously for example in the US you've got whistleblowers who are paid for blowing the whistle. If there's a successful prosecution or regulatory action off the back of it, they get a relatively significant amount of money for having done that. We don't do that in the UK. The SFO have come out and said they don't want to do it. The FCA reviewed it not too long ago and said they don't want to do it. I think everybody has probably a personal view on it. But in terms of protection, there are protections within legislation here in the UK in relation to protected disclosures, i.e. whistleblowing report. The alternatives are to remain anonymous. You don't have to provide your details when blowing the whistle. The difficulty with that is as we've seen relatively recently is firms may well start to try and make enquiries to figure out who the whistleblower is. Not something they're meant to do, and it's not in the spirit of the regime. But yes possibly remaining anonymous through the process is a way of protecting yourself. But there are legislative protections, it's a question of are they being applied? And as you say when you talk about things, how safe do people feel to speak up, to talk out? And it goes back to, as you were saying, culture. GILLIAN: Yes, it's an interesting concept. If the culture of the organisation is open and transparent, then there would be no whistleblowing, right. MICHAEL: Yes. GILLIAN: So it's quite an interesting, certainly an interesting topic, and definitely it leads back to culture. MICHAEL: Yes. PRESENTER: So let's move on to MiFID II now then. And, Gillian, what

have we been seeing since it came into force in January? GILLIAN: Well as I said right at the start I think firms are still, even six months on it's still a bit of a bedding-in period. We're hearing now that the FCA are going to start having a right good look at transaction reporting and really trying to understand the data that's coming through. They had issues right at the start in terms of receiving that data. Firms again are ironing out issues that continue. But with MiFID II, we've got SFTR coming down the line now. I know we're going to talk about that in a little while. So it's so much challenge, the complexity of regulation out there, but I think with MiFID II there certainly still is a bedding-in period happening at the moment. PRESENTER: And, Michael, in June 2018 this year of course the FCA announced that they are to open an investigation into EU directive. So just talk me through what happened there and the likely impact. MICHAEL: Yes, I don't think the FCA were surprised by it, but I think they had concerns that were raised to them by the industry around I suppose how open should you be in terms of pricing or literally accurate disclosure. Andrew Bailey came out and said well look, we can have literally accurate disclosure, but is that in context, does that help the people who are receiving the disclosures to understand how it's operating and how it's working? So they've said they're going to investigate. They said they're going to investigate the impact. I personally haven't seen a lot coming out of the FCA about it. It's something they've said they're going to do. When it comes out, or when an outcome comes out will be interesting to see, but I'm not sure there's been really any great indication as to their progress, or when that's going to be. PRESENTER: And, Gillian, what are your thoughts? GILLIAN: So I think in terms of the investigation I think firms, if they've not already been contacted they'll be contacted soon, and in particular around research costs, because the FCA are keen to understand whether research costs are actually getting passed on to consumers or not. So I think that will be a key focus. And I believe the investigation is going to last for approximately six months. PRESENTER: So, Michael, what are the main issues that advisors face then when it comes to MiFID II? MICHAEL: Got a few, there's a bit of a list: transparency, openness, understanding research costs as we've just spoken about. Also looking at pricing transparency around that, also looking at things such as treating customers fairly, recording of calls, a whole range of things that I think most firms have been pretty good on. Certainly the ones that I've spoken to have got pretty close to being MiFID II compliant, whether or not they're all MiFID II compliant remains to be seen obviously. But yeah I think they're all pretty much getting there, because they've had the run-up time to. PRESENTER: So a lot of information out there to manage then, Gillian. I mean what solutions are available to do this? GILLIAN: I think there's a lot of strong data management and regulatory reporting, as well as anti-money laundering solutions out there. And I think it's, you know, there's been a lot said in the financial press if you like about RegTech, fintech and all that good stuff. So I think actually for some CTOs it's actually quite daunting to decide what to focus on and what technology to look at. But I think aside from that I think definitely firms need to be considering how they can work more efficiently and effectively with data to meet regulatory obligations. PRESENTER: But how can they choose the right solution for them, what should they even be looking for if there's so much choice out there? GILLIAN: I think fundamentally it's about thinking about the data they have internally, also the data they currently get from external sources as well. And really looking, firstly looking at how they work with that data, and then considering can they do it more efficiently and effectively? Certainly what we find with firms is they go so far, and then rely on manual processes, spreadsheets and so forth. Look at the systems you have, can you amalgamate and consolidate that data? Or do you take it into a data warehouse where for example you don't really understand what's happening in that data warehouse, it's a bit of a black box. So it's going back to having transparency of the data, the granularity of the data, and how you can work more efficiently and effectively with it. PRESENTER: So the European Market Infrastructure Regulation as we know it requires reporting of all derivatives to a trade repository, what would you say are the issues with this? GILLIAN: So actually 30th May 2018 the ESMA, the European Securities and Markets Authority, issued their latest Q&As.

And a significant point in there is that with derivatives they're basically saying that position levels, the reporting of position levels under EMIR transaction reporting will be mandatory. And further than that the position has to be reported by both counterparties to the derivative. So that's a significant change for firms. PRESENTER: And so if all of this wasn't enough, we've got the Securities Financing Transactions Regulation. This is coming into play next year, what do people need to know? GILLIAN: So the first thing they need to know is that you're basically, well you're over doubling the data fields required under MiFID II transaction reporting. So for securities financing transaction reporting, you're looking at 153 data fields. Probably you will populate about 65 for transactions there, but again that's a really, that's a lot to take onboard given the amount of work that's already gone into MIFID2. PRESENTER: I suppose there's people out there thinking it's a little bit way off in the future, I don't need to start thinking about that now. What's that mindset, is that OK? GILLIAN: No, we're basically talking 12 months away. So again if I was a firm right now I'd be saying right, what are those data fields, I need to understand what those are. Does it apply to me? Can I get that data? Is it internal, is it external? And lessons learned from MiFID II, really have a look at how your project was implemented for transaction reporting with respect to MiFID II, and really think about lessons learned from that. And hopefully that should be a smoother transaction where SFTR does apply. PRESENTER: So GDPR, it's come into force, we're hearing a lot about it, we're certainly being flooded by emails. How are people getting on with it, Michael? MICHAEL: It's taken a huge amount of work for a huge number of firms. This isn't just a financial services issue; this is obviously a much wider issue than that. So yes a huge amount of work has been done in advisory in trying to support firms. Even our firm itself has been sending out those emails saying can we still email you going forwards. So yes I mean in terms of what firms are at risk of going forwards, I think that the ICO have already said look we're increasing penalties, the risk of a penalty is increasing itself. They have put a lot of resource and time into enforcement, and into increasing investigations in relation to cybersecurity breaches. And not thefts of data, inappropriate disclosure of data, or inappropriately obtaining data or holding data passed the time when you actually reasonably need to retain it. So firms have focused quite a bit on I think understanding, kind of goes to the same point I think around the reporting, is understanding what they've data they've got. Trying to collate it into one place, trying to understand how they can hold it, how long they need to hold it for. We haven't seen any enforcement actions immediately off the back of GDPR, but I think they're coming. They're clearly going to be coming. The ICO over the past 12 months has taken quite a distinct increase in the number of investigations that it undertakes. And the ICO is an interesting body in the sense of they have several powers around breaches, so let's say a fine, all the way through to criminal prosecution for breaches, and with their enforcement team being including for example ex-Manchester CID police officers, so these are guys who for years have done criminal investigations and criminal prosecutions. So it's going to be a pretty interesting time to see what the ICO focuses on over the next 12 to 18 months. PRESENTER: But just to recap there, I mean what are mistakes that you're seeing, are you already seeing mistakes, and what should people really be checking moving forwards? MICHAEL: Yes, the key is what have you got? What data do you hold, why do you hold it? Where is it held? They're the key things really that firms need to be looking at. And starting then off the back of that to come up with a plan as to so if we don't need this part of the data, can we delete it? Does our system allow us to delete certain parts of the data that we hold, or would we have to delete for example the customer as a whole? Can we separate it out? Is one customer for example located on five different databases? It's certainly a potential risk and it happens. And if they are do we need their details on all five databases, or can we take it from certain places, and how do we do that? And this costs, this costs in terms of both financial resource but also time, effort, energy, some new management responsibility, everything else that flows into it. So firms are, and I think there was very much a view potentially of oh well when the date hits, that's it, we're done, and I think firms have

started to realise, have realised almost immediately that that's not the case; that this is an ongoing thing that is taking still a lot of time on top of everything else, on top of all the reporting, the senior managers regime and everything else that's going on. PRESENTER: So then how serious do you think people are taking this? They've sent their emails out, it came into force but do they think their job is done now? GILLIAN: I do think firms are taking it seriously. And as Michael was saying though, this is getting done on top of day jobs. So they're taking it seriously, they're probably still doing more, and I think it's an ongoing piece that will continue. I don't think there's ever an endpoint, and they will continue to potentially improve, find issues, you know, remediate issues as time goes on. PRESENTER: So then on the horizon what are the regulatory things we're going to be seeing that we haven't yet covered? GILLIAN: Well on the horizon we've talked about SFTR, but actually one of the other ones we haven't spoken about today is PSD2, so the revised Payment Services Directive that came into force in January 2018. Now that's very much about data protection as well, certainly about increasing competition between service providers, and the notion of open banking. But the reason I've mentioned that is because initially or at a glance you might think well PSD2 has nothing to do with GDPR. But they've actually got two common themes there. It very much is about data protection. It's very much about giving consumers control of their data. So I don't think the two can be divorced completely. And as I say it's very much about data protection. It's such an important issue now. And going back to your original question there, Jenny, I do believe firms are taking it very seriously. PRESENTER: Well something that might be slightly out of people's hands is cybersecurity as you mentioned earlier. How common are these breaches, what are we seeing, and how usual is it for people to actually report it? Because I know in the past people haven't wanted to report this sort of thing. MICHAEL: There's quite a famous quote, which is there are two types of firm. There's the firm that's been hacked and the firm that doesn't know it's been hacked, and I think that's probably true in the vast majority of cases. I mean these kind of attacks are prevalent. They are affecting a huge number of firms. They're affecting firms all over the world. This isn't just a UK issue. I think in terms of what do we see coming out of that, and whether or not firms are wanting to report it, they have to. They're now in the position of well you must. Because if you don't and it's identified by the ICO or the FCA or somebody similar, then the penalties that are going to flow from that are going to be huge and very significant. To the extent that these could be business closing fines as a result of some of these breaches. Now there's a difference between for example having all the systems and controls you can possibly have in place, and a very clever individual managing to hack through those systems and controls and obtain a small amount of data. That's possibly at one extreme. At the other extreme not having any systems and controls in place, or any controls over what your own staff or employees are doing with the data, and allowing that data then to leave the building in a whole host of shapes and forms, whether it be electronically, whether it be on memory sticks, whether it be screen shots, that kind of thing. So firms have been doing a lot of work around those types of aspects, things that they can possibly control more than others, but I think the key message really is if you think you have an issue, or if you think you've identified an issue, you're going to need to deal with it, and you're going to need to notify somebody around what it was and what your plan is for going forwards. PRESENTER: But say a company is attacked, and they lose data, and then if they report it what happens then, will they be penalised, will it have to be made public, you know, what's the process there? MICHAEL: Yes, a variety of options, but in the majority of cases yes there'll be a report to somebody. And yes potentially it will be made public. I mean we've all seen, I've had emails recently from a couple of very international well-known firms saying we've had a data breach, we believe your data may have been affected. Here's for example a credit monitoring scheme that you can sign up to to assess whether or not someone's potentially taking out credit or committing fraud or identity theft in relation to you as an individual. So that's one of the things that firms are putting in place almost automatically now. Also advertisements, notifications on websites, they're becoming

increasingly prevalent, so the customers are aware. And also then looking at well what's the remediation: how do you fix the issue with the system itself? How did the actual breach happen; can you fix the issue; do you need to shut down a website; what kind of practical steps do you need to take to stop it happening again – all the while, for example if you're a financial services firm, with your obligation to notify the FCA and/or the PRA, having to deal with regulatory intervention, and quite intensive regulatory intervention. When we're talking about things like customers' bank details, customers' employer details, dates of birth, addresses, when you say to the FCA well you guys are the ones focusing on customers and customer protection and treating customers fairly, they're currently all over those types of issue when it comes to that kind of breach, working pretty closely with the ICO, they're both now getting to the point of, in certain circumstances, they'll both be investigating the firm at the same time. And again it goes back to resource and senior management and who knew what when, so a lot of similar overarching themes, but I think it's certainly one of the key areas that I think regulators and financial services firms are focusing on, and will be for the next at least 12 to 18 months if not longer. PRESENTER: So let's move on to CAS then, and was this mentioned in the FCA's business plan, Gillian? GILLIAN: Not specifically, but a lot of the themes that we've touched on already today go hand-in-hand with CAS. And it's absolutely still high on the regulatory agenda for firms. I think primarily for some of the reasons we've already talked about in terms of embracing technology and innovation to be able to truly protect your clients. And I think we all know that the FCA and CAS auditors, they really don't have any appetite any longer for having manual processes, spreadsheets, so on and so forth within a firm's CAS control framework. And when you think about SMCR and the potential ramifications there, if you do couple that with continuing with the manual processes, and not having as robust a CAS framework as you could have, I think firms could be headed for a perfect storm there. PRESENTER: Michael, how do you think the FCA are approaching CAS? MICHAEL: CAS is an interesting one, I mean they focused on CAS and then ramped up their team about, crikey, five/six years ago now I think wasn't it, going from a team of about five or six people all the way through to 40 and more now. So it's certainly something that they are continuing to focus on. I think we've probably seen less enforcement action around client money of late. There was kind of a spate wasn't there I think? GILLIAN: Yes. MICHAEL: And it went a little bit quiet. But I know that certainly they do have a couple of FCA investigations that are either well developed or just about finishing or starting that focus on client money as an aspect of them. It's certainly, yeah, it's an area of focus. I think it's almost one of those whereby I think from my perspective there'll either be a significant breach that will lead to them getting very interested, or it's almost a tie on to other issues that they're looking at. So they'll be looking at something like PSD or MiFID or cyber stuff or financial crime, or whatever it might be, treating customers fairly, and they'll almost automatically now, which they didn't really used to do, tagging client money as something that they'll look at at the same time. PRESENTER: And, Gillian, I just want to look at this Dear CEO letter on crypto-assets, just talk me through what happened here. GILLIAN: So there was a letter went out recently to CEOs where there are crypto-assets, and it's basically reminding them of their obligations under the rules. So crypto-assets by nature are quite vulnerable, they're open to manipulation, and it was very much about reminding CEOs that you have to have really effective risk strategies and risk management systems in place, have an open dialogue with the regulator, and act cautiously or act prudently with respect to crypto-assets. PRESENTER: So then overall, Gillian, how much need would you say there is for automation, and also how much are regulators themselves embracing technology, or indeed should be embracing technology? GILLIAN: Well they themselves, we've talked about this before in terms of the FCA having their own RegTech team now. They have these tech sprints, and again we've talked about those before. But certainly they had an anti-money laundering tech sprint recently, and international regulators were invited along to that. So I think you had representation from the likes of Singapore, Japan, the States, and from European countries as well. I

personally think that's a big message saying regulators are embracing technology, so why shouldn't firms? I don't think there's any, there's no way of getting away from it. If you think about the business plan, if you think about cybersecurity, crypto-assets, all of this goes hand in hand with firms having to really look at technology, look at innovative ways with respect to treating, how they treat their customers. Better products, better services, and of course the overarching piece about data protection. PRESENTER: And in terms of the speed of change of regulation, it is quite tremendous, so I think it's a lot for people to actually deal with without embracing this kind of thing. GILLIAN: Hugely, because the regulation changes and it becomes more complex. But the actual systems that firms are working with, their operational systems, they don't change. And for a lot of firms they've been there for quite some time. So there's kind of an imbalance if you like, as well as trying to, because these are systems that are put in place for operational reasons, not necessarily to meet regulatory reporting or regulatory obligations. So again there is that imbalance. But there's more and more firms and systems coming to market that really can help. PRESENTER: So it's too late though if people haven't perhaps put this in. With everything that's coming up, should they still be thinking about it? GILLIAN: I think actually for future proofing, because I think regulation will continue to change. I mean I mentioned Brexit, we're right at the very start, we don't want to talk about Brexit today but who knows what that will bring. Who knows what change that will bring? And I think it's about firms thinking about the culture. I think culture and tech, if I was to pull two of the priorities out, if you get those right I think it will stand you in really good stead for the future. PRESENTER: Well we are almost out of time, so I'm going to now ask you for your final thoughts, how to summarise this session. Michael, why don't you go first? MICHAEL: I think my overarching thoughts are there are a number of changes coming, there are a number of challenges coming, and I think firms shouldn't forget the work that they've done over the last six to 12 months around the various areas that we've spoken to, and think, going back to the tick list, big tick we're done, move on. I think the FCA business plan and the FCA's approach has been clear that the issues will carry on. The areas of focus are not drastically changing; they're going to continue in the same way as they have done historically. And I think you're absolutely right, technology is one of the key ways of how they're expecting firms to deal with that. The FCA having ramped up its own technology teams significantly over the last couple of years, I mean they're saying that we're doing it, this is where we expect you to get better, and these are the tools we expect you to use. PRESENTER: And I think a lot of people forget, I don't think the FCA are trying to catch people out, this regulation is put in there for a reason. So perhaps it's worthy of remembering that. MICHAEL: Yes. PRESENTER: And Gillian, your final thoughts. GILLIAN: I think actually that's a really good final thought what you just said there Jenny, but I echo what Michael said in terms of tech, and I go back to culture. I think culture within a firm is so important. And it's almost like having that open and honest dialogue within your firm actually could potentially help you having a more open dialogue with the regulator as well. I think regulation will continue to change. I think the speed of change will continue. The complexity will continue. So yes, it's just about firms doing as much as they can to embrace that. And not to stop, just because a deadline has passed, do as much as you can but continue to refine and just learn from the lessons of previous implementations for other regulations as well. PRESENTER: Super, well Gillian, Michael, thanks so much. GILLIAN: Thank you. MICHAEL: Thank you.