**Julia:** **Hello and welcome to a DerivSource Podcast. I'm Julia Schieffer, the founder and editor of DerivSource.com.**

**So we've covered cyber risk in previous podcasts, but today we're discussing identity fraud, where people are opening accounts or doing suspicious transactions under a false identity. Regulation requires that financial institutions know their clients, and as such they must have controls in place to ensure that they know who they are dealing with, so they can better identify suspicious transactions early on.**

**Specifically under MiFID II, firms need to send execution and decision maker details, so the question for firms is "How do you know who the people that conduct the trades are who they say they are and are not necessarily sharing login details or hardcoded logins in static data tables?"**

**In this podcast we're speaking to Ian Bamber of Capital Edge Consulting, to shed some light on the risks of identity fraud and how this impacts institutional financial firms from a regulatory, compliance and risk perspective.**

**Welcome to the podcast Ian!**

Ian: Thank you very much; it's a real pleasure to join you today.

**Julia:** **So, when we're talking about identity fraud, I think of credit card fraud or stolen social security numbers, how does identity fraud impact financial institutions, and who internally, you know which department, tends to be in charge of monitoring this?**

Ian: Well, thank you very much for the question. I think identity management is going to become a topic that you hear more and more about in the coming years across a number of industries. We're of the view where anywhere where a high value transaction is taking place electronically you have the potential for someone to fraudulently identify themselves and then, therefore, fraudulently undertake the transaction when they are not who they say they are. That type of activity can take place just as easily on a trading floor as it can in an office or in a café in the West End of the City of London.

Firms are becoming more aware of the opportunities for people to fraudulently identify themselves, and the bad guys out there are coming up with more and more inventive ways of doing that in a way that they're more difficult to detect. That's an industry problem and you can open the pages of your newspaper pretty much any day of the week and see real world examples where people are having their livelihoods severely impacted or taken away from them by identity theft.

When it comes to the corporate and investment banking worlds and trading, it is also going to become relevant to regulated firms that they feel that they have adequately identified investment decision makers, buyers and buyer's decision makers, sellers, and people that are making decisions where risk is taken and value is transferred. Certainly the current processes for identifying people in many firms relate to usernames and passwords that are captured when people log on to the various trading and risk systems that are used for those purposes. But we believe that in time that will move towards real time identification using biometrics or visual or voice recognition systems, because those systems are available now and they are real time, and they obviously allow firms at a relatively low cost to capture that data about the individual and avoid that people are potentially misusing usernames and passwords for purposes that they are not authorised.

**Julia: Why is it so important to focus on preventing identity fraud in this context now?**

Ian: From a regulatory perspective, in at least my opinion, the regulators are now seeking accountability transparency across the firms that they regulate. What I mean by that- it's not the chief compliance officer or the chief executive, they're looking at when it comes to meeting or missing a firm's regulatory obligation the responsibilities are being delegated and federated across firms for compliance based upon a number of control processes. So there are people in operations that will now be responsible to regulators for the performance of the firm; traders and heads of desk and salesmen are obviously responsible for their actions in terms of advisory, in terms of trading and risk management. And so therefore the responsibility to identify those individuals at the right point in time during the process of undertaking a transaction and then obviously clearing and settling that transaction subsequently is an area where the regulators require more transparency from the firms that they regulate. And that's why we believe that there's a significant amount of interest in identity management platforms because they enable you to capture that information to a much higher degree of certainty than the sort of traditional username/password type approaches and factor identification approaches that most firms are familiar with now.

**Julia: What process do firms currently have in place to identify identity fraud in this context and does it work?**

Ian: You know it's pretty obvious that many firms in the past may have had fairly weak processes for identifying who they were dealing with, either as a buyer of services or a seller of services, and if you look at the MiFIR transaction reporting requirements around buyer decision maker, seller decision maker and investment decision maker executor, you can see that part of the MiFIR reporting obligations are to provide transparency as to ultimately who is accountable for those activities between parties to a transaction. It would not be usual for the HR systems of most firms to be cross-referenced to the trading and risk management systems of the same firm, so a kind of one to one mapping of those individuals doesn't exist in terms of systems that capture that information then subsequently report it.

So I think that a lot of work is going to need to happen in terms of making that connection, in terms of the back-office systems that capture and carry HR information and the responsibilities associated with those individuals and correlating to those systems that are transactional in nature, and obviously making sure that the information between the two is correct and reconciled.

Then you get into a secondary consideration as to can you prove the identity of the individual that's associated with the transaction was actually the decision maker, whether it be a seller decision maker or the investment decision maker, and that's obviously where identity management systems as well as strong linkage with your underlying HR systems will become important.

**Julia: So Ian, are there any better ways that firms can improve this process, and if so how?**

Ian: It's a really difficult question, Julia. I do think this space is one where you will see significant innovation in the coming years. The methods of identifying people electronically are changing very, very quickly; there are applications of artificial intelligence in this space.

For example, if you're having a video conference with a customer, you can use artificial intelligence to look at how their facial expression might reflect their mood. So are they stressed? Are they angry? Are they frightened or concerned? Therefore, if you have that information you might then consider whether or not that person is in a good state to undertake a transaction with you at that point in time. So there's really interesting research going on in this space.

The methods and means of identifying and authenticating individuals are evolving rapidly. There are a number of different methods out there within the industry for doing this, and we're starting to see those technologies come together with technologies that allow you to digitally sign contracts for example, and ultimately with the block chain to sign a contract digitally and obviously immutably prove that with the block chain.

So from my point of view I think there's a lot of noise and discussion at an industry level around "Where is digital going to disrupt the corporate and investment banking world?" I think that block chain is a topic that people know well, but I also think that as the conversation develops and the research and technology grows that you'll see more end to end solutions that would include encryption techniques and cryptographic signing of contract documentation. I think you'll see semantics as a method of unpacking contract information so that it's very clear and unambiguous to both parties to a transaction, and you'll also see identity management as a method of capturing in a sophisticated way in real time the participants that are involved in the transaction.

So I do think it is space that will move quickly. I don't know that it's going to significantly grow the income of the financial services community, but certainly we are of the view that it will significantly strengthen the security of a lot of the processing, and in automating those processes and therefore reducing friction between counterparts who want to transact, then obviously you create the capability if you can transact efficiently to trade more regularly and efficiently.

**Julia:** **Can you tell me how banks are looking to use these types of services in the future?**

Ian: It's a great question. Certainly I'd say two things. I think that in terms of digital identity management, we're certainly hearing a number of market participants talking about identity as a service they would kind of build into their business architecture. This is because there are a number of areas of the business where identity is important within a firm but obviously also important between firms, so several firms that we've talked to are looking at this as a kind of change in the way that they look at their business and look at the capture of customer and employee information. We see that as an area that firms will look at and expand on.

The second area that I think is interesting is that obviously you've got a number of service providers that provide reference information to market participants, and there's been a lot of noise and discussion around collecting customer information and documentation and mutualising it to allow the industry to save money and improve standards. I think if you think about identity and identity management, there is a case to be made for central infrastructures that provide identity management services to regulated firms as a shared service. They would therefore do that to a common standard, they would therefore do that and mutualise the cost of doing so and allow firms to concentrate on their core business as opposed to investing in R&D in technology that isn't their core business but that they can draw upon through service providers that are specialists. And I think that has potential.

**Julia:** **Thank you for listening to this DerivSource podcast.**

**To read the transcript, please go to the show notes page on Derivsource.com.**

**Thank you for listening, join us next time.**