DataShare - transcript of presentation video

Nick:

Here we are, our next team, please give them a hand this is team by the name of DataShare.

Esther:

Good afternoon ladies & gentlemen, my name is Esther and this is Tom. We are from Team DataShare.

Tom: Hi everybody, thanks for coming along today. You can see the figure in front of you here, so I'm going to let you think about that for just a few seconds about what that figure might actually mean, so I will reveal it for you. It's the amount of money that is going to be laundered through the UK in the space of this 8 minute presentation, so of that we can collate that we are only going to find 2% of it. I think we can all agree, its not ideal. So as a Bank, as NatWest we have a problem, we have a challenge as to other banks in this room. We have thousands of alerts, and those alerts we absolutely want to work and take a look at and figure out whether or not we want to do anything with them.

One of the things that we all do as banks and other financial institutions is, we prioritise those alerts based on the information that we have, so there will be certain risks appetites we put in place to put triggers or alerts in a particular order, but what should I prioritise? what could we do better? At the moment, NatWest, as an example, we only have one piece of the information. We only have one profile, we have our customer data, our customer transactions, so we can understand what that looks like, but just imagine what we could do if we all work together to collect that information and we would have a bigger picture of what our customer actually does across the network.

So to bring that to life, you might have a UK based business, its domestically focused, its trading in the UK, domestic payment only, no other obvious risk factors, you might have an alert, that alert is triggered because you have multiple payments to the same individual company as an example, then you might use third party information to cross reference the same customer and you may identify other risk factor such as cross-border transactions or large volume transactions. So ultimately, if you could use that information, if I could have that information as bank, I could use it to prioritise the alerts and then I could focus my resource. 94% agree that intelligent sharing is key, so most of you will agree with me here, so why don't we share more?

This is an example of major incidents over the last few years, I think you can probably guess what the next part is going to be. Data security breaches. It's vital, we have this in place, people don't necessarily trust third parties, but it's extremely hard, especially extremely hard to share that information, the AML data, with third parties. Until today.

Esther: So, we have spent the last couple of days building up a really practical and easy to implement solution for your transaction monitoring purposes. We are able to prioritise everything and clearly understand where to direct your focus. We have a unique skill sets in our team, we have people from Banks, who knows what the problem is, they deal with it on a daily basis, and we have a RegTech company – Dataminer who knows how to build the solution, on top of that, we have a cyber security company – Cybernetica who will make sure that your data is absolutely secure. I'm not going into details about Multiparty computation here, you guys have heard loads about it already, but suffice to say that all the information is encrypted, and the thing is that if you don't have the key, you can't access the data, and you don't have it. Now you can't leak something you don't have access to. This is the on a very basic level, what the system looks like, on one hand we have a number of banks participating in the network, who upload encrypted data via secure API, then in the system, which is between multiple parties, as you assume, a number of calculations are being performed, and the results are then served back to the banks based on a set of pre-agreed queries that banks can actually make. MPC [multi-party computation] and data protection do really go hand in hand, I mean there are lots of additional controls in place on top of the system that actually prevent any kind of potential abuse or leaking of any kind, and also our partner – Cybernetica has long, long experience in working together with different government agencies, and other organisations, so we know that this works and this is actually secure enough.

Basically, we put in a lists of customer identifiers names, date of birth, addresses, some ID documents numbers, but the bulk of it is transactional data. So amongst countries, plus you can add in any existing risk factors that you have for the customer, what you get back is the lists of valuable data points, some of them are more generic, like total turnover, total incoming amounts, but there are also very specific risk flags to look for, we are talking cash deposits, transaction links to higher risks jurisdictions, and also any potential source raised by other participants in the network. So, let's have a look. Ok, this is the regular lists of alerts you will see, when working with transaction monitoring on a daily basis. Now, what you see, if we could re-prioritise these based on external data, you will see that two that are clearly highlighted, meaning that these are actually the ones where the customers are doing something that is potentially suspicious in other banks.

So, Tom, would you find this useful at all?

Tom: So, hold a sec, so what you are saying here is that you've got my original customer with my data, that we articulated as UK domestic payments only cross-referenced with third party data, but now indicates other risk factors that might make me want to focus on looking at those priorities above my other lists.

Esther: Exactly, so if we now look at the customer profile, the snapchat here, suddenly your customer who is making UK domestic transfers, you will also see

in other banks they have made payments to Russia, to Hong Kong, to Singapore, plus there have been two sources raised about this customer in other banks, so what do you think? Is it helpful?

Tom: I think that having that information helps me as a financial institution to prioritise my thousands of alerts and doing it in a way that is more efficient so I can focus my already finite resource to look at the highest likelihood of an alert to come forward, so I can put it into my most skilled set team.

Esther: And the impact is really immediate, you can immediately direct the most high-risk alerts to the most senior team members, you can identify criminal networks as they unfold, you get better prioritisation, better support in your investigations, and eventually what you will get, more recovered funds.

So, let's get started, we are seeking 10 partners for our pilot. Please go ahead and sign up at datashare.dev if you are interested. Thank you.