Tech Launderers - transcript of presentation video

Grant: Good afternoon everybody, so Sree and I are from Tech Launderers and today we are going to focus on a use case around KYC with a specific focus on homomorphic encryption, but we are also looking at privacy enhancing technologies as well. And to start with today I would like to take you through a story and it's the story of Mary. So Mary is a KYC Analyst, she works in an investigation team of a bank and in there, she gets a number of referrals through, from her account opening team.

Now, Mary looks at business accounts and customer accounts. She loves nothing more than identifying suspicious individuals and suspicious banks and suspicious behaviours, but it can be difficult for her to use the data available to find these nefarious characters. So, the data that she's got, we've got the banks own data, we've also got external data available for Mary as well. And really the question we want to pose is there are opportunities to use other data that can support and approve Mary's ability to better discriminate good actors from bad actors?

Actually, I should also say that Mary is passionate about customer service, so actually she also wants to make sure that if there are good customers coming through, that she can push them through the process as efficiently as possible. And Mary and the bank, they also have another couple of big changes at the moment. We can see that money launderers are using complex corporate structures to facilitate money laundering and actually the use case we are going to talk about today is mules.

So, we can see a high increase in a number of mules and actually a number of accounts being used for mules to transfer illicit funds. So, what if Mary could ask a consortium of banks for high value information in a privacy preserving manner. So, again remembering that we are focusing on mules, so these are some questions that Mary would love to ask, so-

How many bank accounts does this customer have anywhere?

How many of these accounts were created in the past month?

How many of those account are dormant for the past 'x' months?

And have you noticed a spike in transactions in the customer's account in 'x' amount period of time?

I'm not reading any more questions, but these first 4 we thought were pertinent to the Mule user case.

So, here we can see Mary has got some enhanced workflow. On the left in her case management system we can see John De Souza. John is an ultimate beneficial owner, we've got John's passport number, we've got his passport ID number and the product that he's applying for is a commercial current account.

So, on the right, we've got 3 options for Mary. So does she open up the account, does she think it safe? Should she refer it for an investigation? Or actually does she just need a little bit more time to analyse it a bit more? So, at the bottom, we want to give Mary another option. Is there that ability to give her more data to make that more informed decision? And we, at this point will take you through to our privacy ring.

Okay. So, what is the Ring? So the the Ring is the world's first de-centralised fully automated AML data exchange that will allow the bank and Mary to query the network with pre-defined KYC questions and in response get aggregated and anonymised result, okay, And not only is this really good for Mary, but it's also really good for the customer. It protects the customer's information, and actually it's also respectful of data protection laws and respective regions around the world. So, to best illustrate this, I'm going to pass over to my friend and team mate Sree.

Sreekanth: Thanks, so think about this as how would Mary ask this questions as, "how many dormant account does a certain passport have in the network?" The way we visualise the network is, it's a group of, consortium of banks or regulators or entities that can answer this question. And the ring member in this case, you know, when they get the query, they would see something of this nature, they would see a query that says, just add the number of dormant accounts that particular encrypted passport number has, and add it to the encrypted result and pass on result to the next member on the ring.

So, it's not bi-lateral, it's more of a ring-based system. And how do we preserve the Privacy? The end Mary only gets an aggregated result without knowledge of who contributed what to the result. The ring members do not know the individual referenced nor any intermediate results and may not be told the identity of Mary's affiliation. How is that possible? This is possible, by really really cool Math, homomorphic encryption, and we have the writers of homomorphic encryption, Kim and Pascal there, in our team.

Is it feasible? Would it scale? We built a small demo, I mean it, it's a short time frame, but you know the expert were able to build a very simple scheme wherein you are able to query a user passport number and choose a type of a question that Mary would like to ask, and in this case, choose a certain ring. And a bank can have certain rings, they can have different affiliations and choose to be in certain rings and yeah magic happens and you know in this case, there is query that goes across the network and you are able to get really valuable results that Mary can then use to further enhance her, enhance her risk evaluation.

So, a typical scenario was near. Mary could do card identification, document verification, ID verification and we believe that it's her part of her workflow where she adds a ring verification, where she's choosing to go across a network of her affiliations, her bank's affiliations, and ask for all the questions that Grant just mentioned and that proceeds on to how she makes her risk evaluation. And

this is not just one time, it could be the due diligence, you know, that happens periodically.

So, what do we gain from here? We gained that, the main advantage is that a new industry-wide infrastructure for privacy preserving data collaboration. There is ability to aggregate data across providers without leaking any sort of information. This is all homomorphically encrypted data that is passed along the network, and we believe it's the first step towards federated intelligence, as you know that you can get aggregated data, there is opportunity to train models and build more intelligence onward. Pass on back to Grant.

Grant: The impact of this can be significant, so it gives a platform that will allow the banks, the regulators, the crime agencies to collaborate. You'll have high detection rate, if we can improve that identification of goods and bads, not only will that help detect more money launderers, more bad actors, but also it would improve that efficiency and that efficiency will make Mary a bit to get through more case and focus on real people that want her time and her skills. But I think the last bit which we need to call upon is, the experience for the customer. If we can get this kind of data to prove that discrimination, you will end up with better on-boarding journey, and hopefully improve conversion rate and revenue whilst looking at, making sure we are trying to do our best to catch the bad actors. So, thank you that's all from us.

Sreekanth: And I would like to add, I mean the most important thing is we also realise that within a certain bank and subsidiaries, within a bank there is this opportunity to share data and not just to think about outside of the the bank. Which we know it's quite difficult, even in today's scenario and that's our team. Thank you so much.