

## Catch the Chameleon - transcript of presentation video

**Nick:** So, this is team Catch the Chameleon. Thank you.

**Linky:** Good afternoon everybody, my name is Linky De Villiers, and I'm presenting Catch the Chameleon to you today. So, right before I start talking about our problem and our solution, I want to introduce two criminals to you John and Danny, and this is based on a real-life story and ongoing investigation today. John and Danny owns three businesses and they are renowned VAT fraudsters and drug traffickers.

These three businesses are typically in the area of scrap metal and wholesale of tobacco and alcohol. The businesses have directors picked by few of their mates, in a little pool of directors. Their fake addresses typically in a residential area or in an industrial area, and the business names are remarkably similar. They are the chameleons I'm going to talk about today. But before I tell you more, I just want to introduce us, I have no idea Nick already told you but we won 4 TechSprints prizes last year and we are returning team member not to compete this year, but to tell you what can be done with the acceleration support of the FCA.

At the end of last year, I finished the presentation with the invitation to say join us in the network to try and break this criminal network and today we are returning as such. We are a network of 5 global banks with 3 technology enablers as well and we are going to present to you what we've done in the meanwhile. The technology solution has only been about 3 months old now, but we already work on quite a few other parallels.

So, what is this Chameleon problem? Say for example, the tobacco company of John and Danny starts laundering the money in this case, through NatWest. After doing a few transactions, they are being found suspicious, investigated and exited. Suddenly, John and Danny thought "hmmm" lets use the DJ scrap metal Company". They go back to Barclays, they knock on Barclays door, and Barclays onboard them because Barclays has absolutely no idea, it's the same tobacco company that was exited for money laundering reasons.

But what if in a network we could share what we know, without actually sharing the data? To gain that information, to start disrupting the behaviour of these type of chameleons in the network. However, there are few hurdles that we found since the past year, since trying to do this real- life scenario and that's why we are back today, to see if there is a way we can overcome these hurdles. So, what's the solution so far? We are solution made by the industry for the industry. Say for example, I am Green Bank. I want to screen for a small medium business enterprise, using this tool. I'm connected with a network of other banks, using block chain technology. I now want to submit a profile of my small medium enterprise through this network of other banks.

My profile of this small medium business identifiers as well as the main controller for this small medium business gets scrambled, it gets hashed and data privacy

enhancing technology- I'm not going to go into details- and that can get distributed with the network. The rest of the network has its own technology which enables them to send us a response on a field by field basis to tell me where do we have correspondences on a fuzzy level and we are not. I could also enrich that response with say, for example, a flag, that could be an enhanced due diligence flag, but that flag is informed by certain risk indicators that sits behind it. Say for example, a customer has been extradited for money laundering before, it could inform a flag to say as the user bank you might want to do further enhanced due diligence and that is what I'm prompted to do now. Suddenly, I know a little bit more about this character, and wonder whether he really is who he says he is and I can go do my homework.

Let's show you what this looks like in a screen recording of the tool so far. So on the left-hand side, you can see the diagram that I just discussed. I have a business, say for example - Susan's hairdresser, I submit to my tool. I use her customer ID because I'm already banking with Susan's hairdresser, I'm doing due diligence on her. I'll check that the information is indeed, Susan's hairdresser that I want to submit and now I submit it to my block chain network.

At this point, all my information gets hashed and scrambled, and it gets passed through the firewalls of the bank, but no real data leaves the bank. The network then sends me a response back, this response at the first glance for the investigator, is an aggregated level, just to show me are there inconsistencies and where do they lie? In this case, you can clearly see, that in the red area, were the businesses and the main controller seems to be remarkably similar across the network. However, I'm not quite sure what I'm seeing here yet, so I might want to know a little bit more.

This information could also be enriched, as I already explained a flag that could be something like an enhanced due diligence flag. All this flag does is, it prompts me to go check my information, not to make a decision, but to say actually 75% of the businesses in this network has raised some sort of risk indicator which would be a common agreement of what that would be- say for example, an exit flag you might want to go looking a bit deeper. Now I can draw down to a deeper level of a business by business and I can see with the businesses that half the gross inconsistencies show up in red and that slider shows me according to my risk appetite. Then on a final gradual level of detail, I can now see on a field by field basis where these inconsistencies lie. So, I see for the main controller there are actually inconsistencies in the red boxes which is the name and the industry type of the businesses.

However, the email addresses seems to be remarkably the same, perhaps the post code as well. Looking at the main controller, I say hang on, the surname and the email is again always the same, but there are inconsistencies in the first name or the date of birth which perhaps could have indicated that these are relatives are the main controller and I can go and do my enhanced due diligence.

So where are we with our collaboration so far? We started the development of the tool about 3 months ago. As I say we have a back-end, a block chain network, a working front end and a privacy enhancing technology. We have a network of 5 banks that already work on collaboration agreements and explore the legal frameworks that we work on. The next step would be to test this technology and the scalability of the technology and also to expand on our legal frameworks and do further investigation and that is why we were here this week to get that valuable input and it's been a successful week in that terms. And then finally, we want to start working on our legal and regulatory guidance and the framework that we want to present this within. I'm now going to hand over to Nigel, to tell us about the future.

**Nigel:** Thank you Linky and thank you to the team who have been working hard over the last few months, especially this week. What Linky has told you about is a tool, a new tool, a new tool developed by the industry, for the industry. A tool that will inform and influence our customer due diligence work and our financial investigation work. A tool that will share knowledge, but protect and not share personal information. A tool that will give indicators of previous money laundering or terrorist finance. In short, and in summary, a tool that will make what is previously unknown or unseen available to us, to work together to prevent financial crime.

It has 3 key benefits, the first key benefit for us is it will make the UK a more challenging environment for those criminal actors that choose to abuse our financial services. The second is it will make efficient and effective use of our resources, enhanced due diligence that we do being focused and targeted where it is needed most, where the risk is highest. And thirdly, in the tool, from things, prosperity and security which will working together contribute to the UK. I have 3 asks for you, that I will ask from this. We've delivered the technology, we've delivered collaboration, we need you to help us get over the hurdle of legal regulatory issues which are eminently doable.