How does the Consumer Data Right work?

So when we're talking about the Consumer Data Right, and the Standards, it's helpful to talk about it in the context of the process that the customer would actually go through and which aspects of the Standards are applicable in each of those stages and steps that a customer would go through in actually consenting and authorising a data recipient to receive data from a data holder and for that data to be actually transferred.

So the first step when a consumer has an intent to or desire to transfer data to a third party is through the third party itself, the accredited data recipient. They had engaged with an app or a service or some sort of thing and they want value from that service and the service then system, well I can add more value if you share with me your data and the customer says I'm fine with that and I trust you as an organisation.

And then there's an engagement that happens at that point to say, okay, I will now share data that is held for me with a data holder with you. The first step in that is actually not API based at all. It happens entirely on the accredited data recipient side and effectively the accredited data recipient will display for the customer, the consumer, what data they want to get, why they want to get it, for how long they want to get it, how often they want to get it, and all of the other aspects of consent that goes forward. So it gives the consumer explicit, clear, transparent guidance on exactly what data recipient is going to get from the data holder about them and what they're going to do with that. There are guidelines around that and they’re mainly to do with Consumer Experience. So the Standards do have guidance in language and presentation, some of which are binding and some of which are guidance, but they do stipulate some constraints on the decider, the recipient for those screens so that the consumer has this consistent experience across multiple data recipients.

The next step is that the accredited data recipient will actually communicate with the specified data holder. So for instance, the consumer said, my information is held at ABC bank. There is a, you know there's a bank that I have an account with and they will select the bank that they have data with, with the data recipient. Then the day the recipient will communicate with the data holder. That communication is governed by the information security profile and it is also governed by industry standards such as the financial API standards and open ID connect, which both of which build upon OAuth2. Specifically the accredited data recipient, at this point will call the authorisation endpoint or the authorised endpoint for the data holder which they've obtained and figure out how to call through using OIDC discovery and the ACCC register.

They will communicate the consent that has been requested to the data holder and then they will wait for the data holder to continue the next step in the process. It should be noted at this point that when I talk about accredited data recipients in this context, it's not an organisation, it's a service or product that has been implemented by an organisation. So an organisation that is accredited with the ACCC may have more than one service that's actually in market. You know, many, many companies will have multiple apps or services or websites that they support. In this context, the accredited data recipient is a technical entity. It's an implementation of the

standards. It's not an organisation, it's a service or an app. So at this point it's, think of it as a fintech.com.au is making this call.

Once the data holder receives the authorisation request from the accredited data recipient, the next step is to authenticate the consumer. At this point, the accredited data recipient has a relationship with the consumer and the data holder has a relationship with the consumer, but they're not sure whether they're both talking about the same person. So at this point the data holder will actually present to the consumer a screen and ask them to put in a user ID and will then send them a one time password through a channel that they're familiar with, which they'll enter and that that will close the loop and then they'll be able to authenticate it. And that's to protect consumers trying to access other people's information. It's a step that's required so the data holder knows exactly whose data they're giving and they know that that person has authenticated themselves so that they're able to give it.

Once the authentication has occurred, the data holder will then present to the consumer, 'hey, this is what's been requested, the data recipient, this is who they are, this is what they've asked for', and effectively that the data holder, the bank will reflect back to the customer all of the information that the data recipient had presented to them previously. And that's an important check to ensure that in the intervening communication there wasn't extra requirements or permissions added in. So the customer gets to see at the data recipient, this is what I'm asking for. And then at the bank end that it's reflected back and the customer's able to say, yes, that's the same thing that I asked for. I will now authorise that so they authenticate and then they authorise the consent. Once that consent has been authorised, the data holder will then communicate back with the data recipient.

When the data holder communicates back with the accredited data recipient after authorisation has occurred effectively what is happening is that the data holder is giving the accredited data recipient a set of tokens. Those tokens represent the consent and authorisation that has occurred. Think of those tokens like passwords. It is now a user ID and password that the accredited data recipient can use to get that consumer's data and only that consumer's data under the constraints of the consent that's been authorised. Those tokens, those user IDs and passwords can not be used to get other consumers data and they can't be used to get data that was not included in the consent that the customer authorised. However, they can be used for potentially a long period of time up to 12 months. This is important for certain use cases where the consumer wants the data, their data to be transferred to the service, continually think accounting software or financial management software where the customer wants every day, any transactions to be sent to the data recipient, but doesn't want to have to log in every day for that to occur. So that user ID and password that those tokens that the data recipient now has that can be used with that specific data holder can be used for up to 12 months.