**From:** Jo Cooper [mailto:Cloudinsurance@outlook.com]
**Sent:** Tuesday, 19 September 2017 4:39 PM

**ID Exchange (formerly Cloud Insurance) input into the Open Data Inquiry.**

**Subject matter focus:  Consumer digital consent practices.**

**Introduction**

With the introduction of many Open Banking Initiatives the risk to customer data increases as it is used to facilitate information exchange across applications and vendors.

Most customers are unaware of how this data is used, where it is stored and who has access to it making it impossible for them to make an informed decision relating to its use, or even if they want it to be shared.

Customers are not clearly informed about the personal information exchanged between two financial applications, assuming tacit consent when in fact this may not be forthcoming if full disclosure of the shared information were made.

The requirement for disclosure of all shared information becomes even more important with the Australian Government’s initiative to establish an open financial framework allowing people to seamlessly use their data across multiple financial services.

Australian citizens must have the ability to control how their data is used and made available, and they must have the capability to easily and effectively manage this.

They require the ability to Opt Out, or Opt In to methods of using their personal data easily and intuitively, otherwise this personal data may be made available in ways they neither foresee or agree to.

The ability to Opt Out and Opt In helps build trust in Open Banking Initiatives by placing control in the hands of the person whose data is being used helping to adopt barriers to adoption.

**How Opt-Out Technology can build trust for Open Banking**

Fintech Australia has reported “between 10-50 per cent of potential customers baulk at handing over their passcode, irrespective of strong security and privacy measures. This significant barrier on customer uptake is discouraging innovation in this area”.

The reasons for this are twofold – the first being that the current, voluntary, ePayments Code does not adequately address customer rights and protections in an open data environment. The second is the frequency of media reported data breaches where customers are “the last to know” and often several months after the fact.

The ability to Opt Out provides the customer with the ability to choose how their data is used and shared and by passing the control to the customer the level of confidence in this new financial frontier builds.

OAIC and other global reports also indicate a growth in “trust” concerns which need to be overcome to ignite the opportunities an Open Data economy can enjoy, but provide the right for users to retract access controls where reputational damage, misuse or data breach has resulted in harm to users.

By providing consumers control with choice so individuals can derive value out of consented data sharing is an approach that we believe will underscore a range of data governance principles and allow easy execution in the hands of the consumer.

FinTech Australia has identified Data Security as one of the keystones for successful adoption of the Open Banking Initiative and clearly stated that “Customers would expect that their data is securely transferred and held when it moves from one financial institution to another financial institution, so that it cannot be accessed by hackers. They would also expect secure storage of this data”.

The missing piece in this statement is the lack of a customer friendly method of Opting Out of having their data held by an organisation that has been the subject of a breach, or one they no longer have confidence in.

This capability, even if unused by the customer, is a key underpinning for their confidence in an area where technology drives innovation and often the ‘human factor’ is lost.

A study carried out by the UK relating to health data showed that while most people were, generally, in favour of their data being shared many had not thought about it and some were against the idea.

It was within this framework that the “UK Secretary of State for Health asked the National Data Guardian to develop a consent/ opt-out model which makes it absolutely clear to patients/users of care when health and social care information about them will be used and in what circumstances they can opt out.”

Developing an equivalent financial capability will help to build broad based community support for Open Banking and the associated data sharing required for successful adoption and acceptance.

To this end the Seven Caldicott Principles highlighted in the “National Data Guardian for Health and Care review of Data Security, Consent and Opt-Outs” report published in June 2016 are equally valid when applied to the Open Banking Initiative.

They are:

**Principle 1: Justify the purpose(s)**

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

**Principle 2: Don’t use personal confidential data unless it is absolutely necessary**

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

**Principle 3: Use the minimum necessary personal confidential data**

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

**Principle 4: Access to personal confidential data should be on a strict need-to-know basis**

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

**Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities**

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**Principle 6: Comply with the law**

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

**Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality**

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The ability to Opt Out, or Opt In, as a customer tool is a key foundation to building trust in an environment where the Australian public are being asked to allow many organisations to share sensitive data.

It is incumbent on this initiative to have the highest level of trust to facilitate adoption and this level of trust will be facilitated by providing the customer with an ability to ‘shut the door’ to a threat to their data or their privacy by Opting Out.

Equally their ability to Opt In once the perceive threat is diminished or eliminated provides a commercial initiative to Open Banking participants to address the threats in a transparent, open and public manner.

We also make the following key observations:

* Consumers need more education on being a digital citizen.
* Data sharing from the A end (Credential owner) to B end (Data holder) should also accommodate the end users being the B end, this supports evolving self-sovereignty models in the innovation pipeline.
* Principles for data sharing in the Banking community should be aligned to other sectors so that there is common standards that promote cross sector innovation and data collaboration.
* Power of Attorney/Proxy management + verification frameworks for guardians and others who require **assisted consent** is clearly defined, as our vulnerable citizens can be those first targeted by bad actors.
* Small Business operators face similar data rights/use challengers as consumers when it comes to cyber-attacks, misuse of data and understanding how to be best practice without onerous implications.    Open Banking should also provide the same level of opportunities via incumbents or new FinTech services to assist SME’s to evolve and thrive as digital operators.
* Transparency on the use and terms of data sharing must be in plain English with the value proposition clearly communicated.
* Commercial test, POC’s, sandpits and collaboration with Government API’s for consent hand-off’s needs to be more forthcoming.

We thank you for your continued efforts to enable an enhanced digital environment for today’s and future generations.

Please contact me directly if you require any further information.

Kind regards,

**Jo Cooper**

Co Founder – Managing Director

*Note: We are currently in the process of our Company name change & rebrand.*

**ID Exchange Pty. Ltd. (formerly Cloud Insurance)**

Stone & Chalk FinTech Incubator - AMP Centre

Level 2, 50 Bridge Street -  Sydney NSW 2000

E:  cloudinsurance@outlook.com

M:+61 (0)400 770 147

W: [www.cloudinsurance.com.au](http://www.cloudinsurance.com.au/)



This email communication could withhold confidential data information of ID Exchange Pty Ltd ACN 161437681 (formerly Cloud Insurance).   As such we request that if you are not the correct recipient of this communication that you must not therefore copy, keep, relay or rely, use, copy, save or forward this email distribution or communication.   Unauthorised actions relating to this communication is prohibited and therefore if by chance you have received this in error please immediately discard this email and reply to the email sender to advise of the incorrect address delivery.   Again please delete the received email communication and reply upon sending.