ATTIC
RESEARCH
INSTITUTE

Valuing our Identity

Published on February 14, 2020 by Adam Hunt

The KiwiSaver scheme data breach that was revealed last week was really just a matter of time: I feel for them, they just happened to be first, but it's no excuse. There's a telling statement that keeps being repeated in the media that I think goes to the heart of the problem:

> *Money invested with the company is safe because it's held in a separate system to the one which was breached.*

Let's think about that: the core financial system was safe, but the one holding your personal information was not. That implies that more value is placed on the money than the information. Is that right?

It is a problem I see every day. Frankly it scares me how copies of important and sensitive information have proliferated under our AML/CFT legislation. I've written about this before: the penalties for inadequate record keeping far exceed those for storing too much. Capturing and keeping information you don't need is a breach of Privacy Principle

#1. Failing to look after it is #5.

I know of reporting entities that routinely share detailed outcome reports that include copies of passports, accounts and other very personal information. The customers have theoretically given consent, but do they really understand what this means? These documents collate a detailed customer dossier in one tidy package that gets handed from one reporting entity to the next. And the way it is done is all about protecting the reporting entity, not the customer. Who is looking after customer interests in this relationship?

I think the AML Audit 'profession' also has much to answer for. Reporting Entities must be audited every two years for compliance with their programme. It's a young industry with basically no professional standards and a wide variety of knowledge and abilities. And most of those auditors have little grasp of the overlapping requirements of other laws, especially the Privacy Act.

I commonly see audit findings stating that the reporting entity is failing to keep its own copies of enough information, but they never mention the other side of the coin: privacy. There are other, smarter ways to manage this that are fully compliant. But this lazy, amateurish thinking still pops up time and again. Reminder: you can fire your auditor if they fail to demonstrate competence.

I'm hoping this breach will be the trigger we need to tackle this glaring mis-fire in the legislation and guidance. We urgently need to tackle the proliferation, and somehow get the message out there that privacy can be managed alongside good customer due diligence processes.

* For the record: The TIC Company uses an Enterprise class software solution as used by banks and governments all over the world. We prioritise customer rights over client convenience. We take express consent seriously, even when it irritates our clients. And we don't store or supply multiple copies of documents: we re-use and link whenever we can, and only grant access when there is good cause, such as an audit or an FIU request.