

ATO will add security layer to agent linking

TECHNOLOGY

Second commissioner Jeremy Hirschhorn says nobody can afford complacency in the wake of Optus and Medibank hacks.

By [Philip King](#) • 21 November 2022 • 5 minute read

The ATO will embed a fraud prevention layer into its agent linking system to raise security in the wake of extensive GST fraud and the recent hacks of Medibank and Optus.

Second commissioner Jeremy Hirschhorn said both the ATO and tax agents were entrusted with extensive personal information and cyber criminals were getting more sophisticated.

“If Optus and Medibank tell us anything, it's that nobody can afford to be complacent,” he told the IPA National Congress at Surfers Paradise last week.

“Operating in an increasingly digital environment means that we have to consider how we safeguard our systems from ever-evolving cyber threats and fraud attempts.

“And fraud is not only just about money, but it's also about information.”

“We're entrusted with protecting the community's personal information and this trust underpins the whole tax system. But at the same time, we provide you as tax agents with trusted access to those data stores for your clients.

“You yourselves hold very significant data on your clients. So we've begun a fundamental shift towards embedding fraud prevention measures into systems as part of the initial design process.”

He said the extra security would involve changes to the way tax agents interacted with the office.

“To protect your clients, we may need you to do more, or to do things differently. One area where you'll see this play out now is around agent linking.

“We have been seeing increasingly sophisticated efforts by criminals to impersonate legitimate users to lodge fraudulent returns or gain access to data that they can make money from.

“And in many cases, that is through exploiting tax and BAS agents.

“So that is why we have to boost our front-end controls.”

He said the new system would align the ATO more closely with best practice and would be rolled out progressively, starting with larger businesses.

“Following a successful pilot involving about 40,000 entities and 800 agents, we're changing the process for an agent to link to a taxpayer's account. This is to help ensure that only a client-authorised tax agent as agent or payroll service provider can link to their accounts and access their tax and super affairs.

“Agents involved in the pilot told us that their experience was relatively simple, but we are looking for ways to make it simpler.

“For clients who aren't already connected to online services for businesses, we recognise that there are additional steps involved to transition clients into a digital environment.

“But over time, this will have to apply to all taxpayers.”

Mr Hirschhorn said the office had learned from large-scale GST fraud that a system set up to pay refunds “almost immediately” was vulnerable, and it had changed the process to make it more secure.

“Since we've changed our settings, we've blocked over \$2 billion of fraud attempts before the frauds have been paid out.”

He acknowledged that there was a tension between the security of an interaction and the need to make speedy refunds to legitimate businesses.

“So there's a real challenge of how do you have the safeguards against the safeguards?”

But repeated a warning about the scale of attacks on the ATO – equivalent to almost one a second, or 3 million a month – and said the office valued its high satisfaction rating by the public highlighted in the recent Trust in Australian Public Services report.