ATO Requirements for Software Companies – 2FA/MFA

Introduction

If a Digital Service Provider (DSP) – best understood to be a software company – provides a software product or service that reads, modifies, or routes any tax or superannuation related information, then that DSP is in scope of the ATO Operational Framework. This includes DSPs that use an intermediary (such as a gateway or sending service provider (SSP)) to interact with the ATO.

Context

This update is only about the 2FA (2 factor) or MFA (multi factor) authentication requirements. For the purpose of this document we will use the term "2FA".

ATO requirements

1. If the product is hosted by the business (desktop, on premise, own server): 2FA is optional according to the ATO requirements.
2. If the product or service is hosted by the DSP (cloud, browser based, DSP hosted, accessible from any device type): **2FA is *mandatory***.

Impact on the DSPs

Software that has the mandatory requirement must implement and mandate a 2FA solution for all users with access to tax or super related information.

The proposed implementation date for the DSP to have this option is:

- For tax practitioners' products:
  available by 31st March, 2018 and mandated use by 30th June, 2018.
- For products with access to large volumes of tax and super data:
  available by 30th June, 2018 and mandated use by 30th September, 2018.
- All other mandated products:
  available by 30th September, 2018 and mandated use by 31st December, 2018.

Alternatively they must provide assurances that sufficient controls are in place to mitigate the risk.

Moving into the future the government will develop the Trusted Digital Identity Framework (TDIF) which may alter (hopefully improve) the software and user experience as it replaces the Cloud Authentication & Authorisation solution (CAA) that is based around AUSkey, Access Manager and the Unique Software ID.

Impact on you and your clients

The burden is on the software companies to deliver this solution to us.

If your software is unable to implement (or obtain an extension from the ATO) you may lose the ability to lodge tax and super information, or retrieve information back from the ATO through that software.

MYOB, Xero, and Intuit QBO all have 2FA solutions available.

ICB Comment

We believe 2FA is a mandatory requirement for all business software – any software that has access to the business records or personal information, whether it is provided as a desktop, hosted or cloud-based application.

As professional bookkeepers we are protected if better security is in place on our software, and also on that of accessing client data.

The ATO are solving part of the problem and are able to mandate a requirement within their regime. As professionals we should require it of the software we use and recommend.

The ATO are increasing other areas of the security around the DSPs. Further information will be provided by ICB to you about the impact of these requirements on the software solutions we use, in future months.

References

- ICB – Multi-factor Sign-in Will be Compulsory
- ICB – Upgrade Your Software Or Else…