Key Outcomes

Title:	Operational Framework Review – Fraud Detection & Monitoring Focus Group		
Issue date:	2 December 2020		
Venue:	WEBEX		
Event date:	13 November 2020	**Start:** 10:00	**Finish:** 12:00

Chair:	Diana Porter	**Facilitator:**	Diana Porter Jarrod Wellings
Contact	Diana Porter	**Contact phone:**	(02) 4724 0528

Attendees: names/section	ATO Kylie Johnston - Director, Digital Partnership Office Anu Duggirala - Director Digital Wholesale Integration Claire Miller - Director, Digital Communication & Identity Services Diana Porter - Digital Partnership Office Fiona Homan - Director, ICS Security Governance Mark Macdowell - Director,Digital Communication & Identity Services Jarrod Wellings - Digital Partnership Office Industry Artur Czernecki - ELMO Software Clyde Netto - Thomson Reuters Craig Booth - Ascender Pay Estevan Chaves - Sage Software Australia Grant Christensen - SuperConcepts Helen MacGillivray - Xero James Cameron - Superchoice John Paul Lonie - IRESS Josef Bobinac - Ozedi Holdings Matt Lewis - Intuit Matthew Prouse - Xero
Apologies: name/section	Toby Amodio – Director, IT Security Claire Miller – Director, Digital Communication & Identity Services

	Nick Kelly - Digital Communication & Identity Services Andrew Smith - MYOB Australia Andrew Strong - AMP Brett Reed - e-Payday Kim Sung Do - BT Financial Simon Hutchinson - Reckon

Next meeting	TBA

The key outcomes for this meeting are best read with the fraud detection & monitoring focus group presentation.

Agenda item: 1 – Introduction & Overview

An overview of the findings from the independent review and DSP feedback included 3 opportunities to investigate and improve information security documentation relating to fraud.

These include:

1. Expanding security monitoring control
2. Preservation and retention of audit log data
3. Breach Notification Guidance

Agenda item: 2 – Expanding Security Monitoring

Discussion on expanding scope of security monitoring control to all DSP controlled cloud environments, including exploring benefits risks and considerations.

Key points from industry discussion and feedback included:

- Commercial impacts to be considered for smaller DSPs in expanding the control.
- General sentiment on uplifting requirements to expand security monitoring is ‘It is good for industry’.
- Sharing security information or having a threat dictionary could assist DSPs in applying specific controls.
- ATO should establish the baseline controls, but DSPs are best placed to determine the level of controls above baseline within their environment.
- Another approach is to align security monitoring practices to business outcomes.

Agenda item: 3 – Preservation and retention of audit log data

The group discussed improving guidance on:

- protection and preservation of audit logs
- retention periods that align to legislative requirements
- accessing information to share in the case of a security incident

Key points from industry discussion and feedback included:

- Current audit logging requirements do not align to those in the breach notification.
- Requirements and fields captured should be differentiated between environments e.g. SaaS vs desktop.
- ATO should be more specific on expectations i.e. should logs only include those related to tax/super interactions? What about third parties/partner apps or other actions within software including payroll/accounting. A clearer definition of tax or super data is required.
- Audit log requirements would be clearer if they were mapped to specific industry standard controls.
- ATO should define baseline requirements and include guidance to help DSPs make risk-based decisions for audit log preservation and retention.

Agenda item: 4 – Breach Notification Guidance

The group discussed opportunities to improve the breach notification process and guidance to assist DSPs:

- to respond to breaches.
- to notify and report a security breach.
- with incident response and fraud investigations.
- with supporting information for clients

Key points from industry discussion and feedback included:

- There is no current mechanism for sharing information or outcomes between the ATO, DSPs and third-party ecosystems when a security incident occurs. Recognising specific details could breach privacy laws could any generic information be shared or any other alternative.
- The term “immediately” is not always practical and should align to an industry standard e.g. APRA CPS 234 sets 72 hours. A risk based model could be considered for reporting a breach based on pre determined factors.
- Clarity and guidance is required on risk thresholds e.g. What type of event constitutes a notification? (confirmed vs. suspected).
- Relationship between DSPs and their non-standard contractual clients around data breach notification may delay reporting and should be considered when providing guidance.
- DSPs want clarity around what the ATO will do with the information provided as a result of a breach.
- ATO to explore the alignment of the Security for Critical Infrastructure Act 2018.

Agenda item: 5 – Wrap Up & Next Steps

Outcomes of working group to be published and circulated, members encouraged to provide further feedback and comment.

ATO will establish a second meeting in December.