

Explanatory Memorandum materials: Application of principles-based obligations to regulated sectors

The table below outlines activities regulated entities may undertake to satisfy relevant anti-scam obligations. Note the activities listed below is not exhaustive and merely a guide.

Regulated sector/service	Example of a scam	Examples of Principles-Based Obligations in Action					
		Governance 58BB-H	Prevent 58BI-L	Detect 58BM-L	Disrupt 58BQ-U	Respond 58BV-Z	Report 58BZA-E
Banks	s 22						
Telecommunication provider							

Regulated sector/service	Example of a scam	Examples of Principles-Based Obligations in Action					
		Governance 58BB-H	Prevent 58BI-L	Detect 58BM-L	Disrupt 58BQ-U	Respond 58BV-Z	Report 58BZA-E
Social media service	A cryptocurrency investment advertisement appeared on a social media service's feed. Upon examination, the cryptocurrency is non-existent, and it involves deceiving victims to enter their personal details on a fake exchange platform.	s 22	The service should alert its consumers, via public posts, to urge caution on providing personal information online.	The service should have algorithms in place to identify suspicious businesses and account holders.	The service should have mechanisms in place to ensure that verified fake advertisement will be flagged with consumers and taken down.	s 22	
Paid search engine advertising service	A consumer is searching on the internet for an opportunity to volunteer. Upon inputting key terms into a search engine service, the consumer clicks on the first output that takes them to a volunteering organisation's website they are interested in joining. When reading the site, the consumer discovers the physical address is fake and is not appropriately registered.		The service should make available information on current scam activity on its service and how it is managing the risk.	The service should implement processes that verify website advertisements displayed on its service.	The service should suspend the suspected advertisement on its service and undertake an investigation to confirm it is a scam.		
Direct messaging service	A scammer impersonating as a recruiter sends a message on a direct messaging service, offering a lucrative job opportunity, flexible working conditions and immediate payment of a sign-on bonus. The number is unknown to the consumer and the message includes contacting an international number, on a different direct messaging service for more information.		The entity should provide regular warnings to consumers be scam aware on its services.	The entity should trace unusual communication patterns within its service.	The entity should have processes to terminate user accounts that frequently share scam content.		