



Level 24  
1 York Street  
Sydney, NSW 2000  
paypal.com.au

7 June 2018

General Manager, Policy Development  
Policy and Advice Division  
Australian Prudential Regulation Authority

By email: [PolicyDevelopment@apra.gov.au](mailto:PolicyDevelopment@apra.gov.au)

Dear Sir/Madam

### **Information Security requirements for all APRA regulated entities**

PayPal Australia Pty Ltd welcomes the opportunity to provide a submission on APRA's draft CPS 234 Information Management Standard.

PayPal would like to provide comments on the following two areas:

- Notification to APRA of material information security incidents; and
- The application of this standard to third parties not already captured as service providers of outsourced material business activities under Prudential Standard CPS 231.

### **Notification to APRA of material information security incidents**

To ensure consistency of reporting compliance internationally, PayPal recommends that the timeframe for reporting an incident be extended to 48 or 72 hours. Further, given the size and complexity of some reporting entities, PayPal recommends that further guidance be provided to determine the "reportability" of an incident – taking into account detection, time to containment and thresholds.

As with all reporting entities, once an incident is detected a response plan requires focus on containment and mitigation to stop the impact from increasing. Upon mitigation, resources can then be directed to forensics, impact confirmation and reporting. Based on similar standards implemented across the world we believe that it is reasonable to expect a 48-72 hours turnaround from the point of impact confirmed (not incident start). It is PayPal's view that this offers the right balance between providing a sound report and ensuring the availability and protection for customers and the organisation.

PayPal also recommends consideration be given to determining a threshold for reporting incidents like the European PSD2 requirements. Establishing a threshold for reporting enables a company to differentiate between incidents (for example the difference between one account takeover vs 1000 ATOs).

**Internal audit requirements for third parties not already captured as service providers of outsourced material business activities under Prudential Standard CPS 231.**

Extending the definition of "information assets" to those not currently captured under Prudential Standard CPS 231 means a wider range of third party providers of web based software applications in areas such as payroll vendors, contact management programs, human resources and marketing applications, and other external providers such as document verification services will be covered by the new Standard.


The internal audit requirement to "assess the information security control assurance" provided by a third party will likely require an amendment to current contractual arrangements to enable this to occur. This places an unnecessary burden on the resources of the reporting entity and the third-party provider, and is a significantly higher level of requirement than those defined in CPS 231.

PayPal recommends that the internal audit requirements be amended to be consistent with the internal audit requirements contained in Prudential Standard CPS 231.

If you require further information with regards to this submission please contact our Director, Government Relations Kate Schulze [kate.schulze@paypal.com.au](mailto:kate.schulze@paypal.com.au)

Sincerely,

**Neil Matthews**  
Chief Executive Officer  
PayPal Australia Pty Ltd

  
Level 24, 1 York Street  
Sydney NSW 2000  
ABN 93 111 195 389  
AFSL Number 304 962