Australian Banking Association

Senate inquiry into the adequacy and efficacy of Australia's AML/CTF regime

Questions on Notice

Question on Notice 1

Senator O'NEILL: I have a few questions that you might need to take on notice. Firstly, could you find out how much the banks have invested per annum since 2013 as a lump sum in meeting the FATF requirements?

Mr O'Shaughnessy: I'm happy to do so.

Senator O'NEILL: Could you do that for that period—and per annum, so we can see if there's been an escalation. I suspect there was quite a significant investment post the AUSTRAC cases regarding Westpac and the National Australia Bank, and technology changes will have led to different opportunities. I'm keen to understand those figures per annum, particularly by institution, for Westpac, Commonwealth, ANZ, NAB, Macquarie and St George—because they're the biggest ones—to get a sense of the scale, the cost and the degree of activity that's happening.

ABA Response - QON 1

The four major banks have recently provided this information in response to Questions on Notice arising from the House of Representatives Standing Committee on Economics - *Australia's four major banks and other financial institutions.*

The ABA does not have access to this data from our members.

Question on Notice 2

Senator O'Neill: Given the importance of detection and given evidence we've had today about how important it is to have CEOs and board members cognisant of responsibilities, even being personally responsible for making sure that AML/CTF requirements are adhered to, I want to point to an article by Charlotte Grieve in the *Sydney Morning Herald* on 27 August this year which talked about incentives to cut corners when the employment of contractors becomes a financial risk. I recall evidence that we received during the auditor's enquiry that banks were sometimes actually just bringing in staff from an auditing company, with the auditing company making claims that they had high-level counterterrorism finance analysis skills, which were found to be somewhat lacking. Is it important to have staff within the bank carefully monitored, perhaps even with KPIs, to make sure that they are doing their work properly, rather than leaving it to chance and external contractors coming in?

Mr O'Shaughnessy: I'm not aware of that article. I'm afraid I can't comment without reading it.

Senator O'Neill: We might send that one to you on notice, Mr O'Shaughnessy, just to get your view.

Mr O'Shaughnessy: No problem.

ABA Response - QON 2

The analysis of the investor advocacy group, the Australasian Centre for Corporate Responsibility, as highlighted in the media article by Charlotte Grieve in the *Sydney Morning Herald* on 27 August 2021, covered 37 of the country's 100 largest listed companies. None of the 37 companies covered were banks or entities within the financial services sector. Accordingly the ABA does not have a view.

Generally speaking, the three lines of defence is a popular assurance model that has grown in prominence over the last decade, and is widely used in Australian banks to mitigate the risks highlighted by the media article in question.

The first line of defence is management control, which involves front-line employees; the second line comprises risk and compliance professionals; and the third is composed of internal audit departments and, often, the board.

Question on Notice 3

Senator O'NEILL: The bank accounts that are being sold on the dark web, what's the scale of that? Is that a new place that money laundering is occurring?

Mr O'Shaughnessy: I understand the question, but I'm not sure quite what you're referring to. Are you referring to an article or a paper?

Senator O'NEILL: No, nothing in particular, but I understand that there are reports of Australian bank accounts being sold on the dark web.

Mr O'Shaughnessy: I'm not aware of that report. I'm happy to take that on notice and have a look at that for you.

Senator O'NEILL: Thank you. It would be good if you could do that and find out a little detail about how that is detected and what has been going on with that, and whether there's a threshold for reporting customer accounts on the dark web to the privacy commission or the Australian Information Commissioner.

ABA Response - QON 3

The Office of the Australian Information Commissioner (**OAIC**) is the independent national regulator for privacy and freedom of information. A data breach happens when personal information is accessed or disclosed without authorisation or is lost. If the Privacy Act 1988 covers an organisation or agency, that organisation or agency must notify affected individuals and the OAIC when a data breach involving personal information is likely to result in '*serious harm'*.

The OAIC Notifiable Data Breaches Report highlights how the OAIC expects entities to prevent and respond to data breaches caused by ransomware and impersonation fraud.

The OAIC received 446 data breach notifications from January to June 2021, with 43% of these breaches resulting from cyber security incidents.

Data breaches arising from ransomware incidents increased by 24%, from 37 notifications last reporting period to 46.

Other key findings of the OAIC:

- Malicious or criminal attacks remain the leading source of data breaches, accounting for 65% of notifications.
- Data breaches resulting from human error accounted for 30% of notifications, down from 203 to 134.
- The health sector remains the highest reporting industry sector (19% of all notifications), followed by finance (13%).
- The number of notifications varied across the reporting period, ranging from 45 in January – the lowest monthly total since the Notifiable Data Breaches scheme commenced – to 102 in March.
- 91% of data breaches involved contact information, making it the most common type of personal information involved in data breaches.
- 93% of data breaches affected 5,000 individuals or fewer, with 65% of breaches affecting 100 individuals or fewer. 44% of breaches affected between 1 and 10 individuals.
- 72% of entities notified the OAIC within 30 days of becoming aware of an incident that was subsequently assessed to be an eligible data breach.