



8 September 2021

Our Ref: A39170817 48.1

Enquiries: Trish Blake, [REDACTED]

Department of Home Affairs  
By email: [techpolicy@homeaffairs.gov.au](mailto:techpolicy@homeaffairs.gov.au)

Dear Sir/Madam

### **STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES**

The Department of Mines, Industry Regulation and Safety – Consumer Protection Division (Consumer Protection) provides the following submission to the Department of Home Affairs discussion paper on *Strengthening Australia's cyber security regulations and incentives*.

Consumer Protection is responsible for administering a number of key pieces of legislation within Western Australia to ensure a fair, safe and equitable marketplace for consumers and businesses alike. This includes the Australian Consumer Law (WA) as well as industry specific licensing regimes and trading standards in the real estate, settlement and automotive industries, amongst others.

Consumer Protection also operates WA ScamNet ([www.scamnet.wa.gov.au](http://www.scamnet.wa.gov.au)) through which consumers are forewarned about scams and are provided with the opportunity to report scams. WA ScamNet monitors scam activity and provides guidance to consumers through public awareness campaigns about current scam trends. In the course of this work, WA ScamNet often identifies areas that could be improved to offer better protections to ensure Australians are better protected from scams.

Consumer Protection's submission is informed by our work in these areas and the need for all regulators to be responsive to emerging trends, particularly when it comes to cyber security as an area of ever-increasing complexity and sophistication. The submission will focus on two key areas raised in the discussion paper; health checks for businesses and clear legal remedies for consumers.

## CYBER-CRIME AND PAYMENT REDIRECTION SCAMS

Consumer Protection has received an increasing number of reports relating to payment redirection scams impacting Western Australian consumers and businesses. These scams have resulted in a substantial amount of money being redirected from a legitimate source to an illegitimate source, generally through email correspondence being intercepted on one side of a transaction. Once the funds are deposited into the scammer's account, the funds are often moved quickly to a multitude of other accounts, making funds almost impossible to recover.

The below table contains year on year data of reports received by ScamNet and demonstrates a growing trend in the number of successful cyber-attacks leading to payment redirection scams.

Year	Amount Lost	Number of Victims
2017	\$461,500.00	5
2018	\$591,306.57	15
2019	\$1,420,350.69	17
2020	\$726,243.93	39

The Australian Competition and Consumer Commission's (ACCC) ScamWatch reports that payment redirection scams were the most financially damaging scams for Australian businesses in 2020 with combined losses reported totalling more than \$128 million. This total includes a number of different types of 'false billing scams', the largest category being payment redirection scams with 1,300 reports and \$14 million in losses. A substantial increase from \$5 million in losses and 900 reports made in 2019.

The below table identifies data published by ScamWatch on the breakdown of all scams in 2020 by business size. This table demonstrates that Micro and Small businesses require additional support, but also that larger businesses may not be willing to report incidents due to fear of reputational damage.

Business size	Number of reports	Reports with loss	Reported losses
Micro (0-4 staff)	1,304	173	\$2,057,087
Small (5-19 staff)	1,056	153	\$4,950,593
Medium (20-199 staff)	651	90	\$1,578,852
Large (over 200 staff)	321	29	\$9,031,213
Size of business not provided	852	49	\$783,418
Total	4,184	494	\$18,401,163



Traditional campaigns to reduce the impact of payment redirection scams and cyber-crime have focused on getting consumers to improve their own practices. These campaigns have included a focus on encouraging consumers to verify bank account details with the trader to confirm any changes and raising awareness about the prevalence of email scams. These campaigns have perhaps been successful to a large extent in preventing even more people from becoming victims to scams. However, these measures alone are proving increasingly ineffectual as the scams have become more sophisticated over time. In a recent case that Consumer Protection is aware of, a consumer attempted to purchase a Tesla online and received an email with a PDF invoice attached. This email was also received by the consumer's financial adviser. Scammers intercepted the email received by the consumer and replaced only the PDF in that email with their own. The Financial Adviser's email remained with the correct invoice from Tesla. This sophisticated scam resulted in significant financial losses for that consumer. In order to combat the increased sophistication of cyber criminals, Government will need to partner with business in order to achieve better outcomes in this area.

## HEALTH CHECKS FOR SMALL BUSINESSES

### Consultation Questions

23. Would a cyber-security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?
24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?
25. If there anything else we should consider in the design of a health check program?

Consumer Protection is broadly supportive of a Commonwealth led health check for businesses. This health check should assess and accredit a business's cyber security and readiness to respond to cyber-attacks in order to improve standards across the economy as a whole. This system will assist Consumer Protection in improving standards across regulated industries, including real estate, automotive and construction, who have become significant targets for cyber criminals due to the large number of high value transactions.

In order for such a system to work effectively, it will need to be comprehensive and proportionate to the nature of the threat it seeks to prevent. The introduction of this system should be phased in with a transition period prior to becoming mandatory, beginning with targeted industries such as those mentioned above.

This health check could occur as a "tick style" system, which signals to consumers that the business has been accredited as having adequate cyber security in place. The health check must only be given to businesses that meet a high standard of cyber security, which is a standard that incorporates a reactive and proactive approach to cyber security. Any health check provided to businesses must be comprehensive in nature and assess a number of key components of a business's cyber security. Specifically, it should consider the nature and scope of the businesses:

1. cyber security infrastructure, including the security of its payment methods;
2. cyber insurance policy, including options for redress for victims; and
3. critical incident response plan.

The criteria for assessment must be clear, measurable and objective, with the results remaining transparent to consumers and business. Consumer Protection suggests that the adoption of an existing cyber security model such as the Australian Cyber Security Centre's (ACSC) Essential Eight may be the preferred option rather than seeking to develop new standards.

### ***Scalable Health Check System***

Consumer Protection considers that the health check should be principles based or general in nature to ensure broad application across a wide range of industries. In contrast, industry specific issues could be addressed by relevant state or territory legislation. For example, conditions could be imposed on the licenses of regulated industries requiring the uptake of cyber insurance, or mandating participation in the health check program.

A scalable system could utilise tiers of accreditation such as a gold, silver or bronze level of cyber security accreditation where each tier increases the accreditation requirements. One such example of where this approach could be beneficial would be in the real estate industry where Consumer Protection has seen a growing number of incidents of payment redirection scams. Each level of accreditation would set minimum requirements to be met, with each ascending level satisfying all requirements of that level and those below it in order to achieve that level of accreditation:

- Gold – Holder of an appropriate cyber liability and privacy protection policy and cyber-crime policy;
- Silver - implementation of secure payment methods to provide an added layer of protection when compared with electronic funds transfer as well as implementation of secure industry specific platforms such as PEXA key or Secure Exchange; and
- Bronze – implementation of ACSC's Essential Eight and development of an incident response plan.

The adoption of a scalable system, which will allow consumers to readily identify and compare the cyber security standards of each business would achieve this aim. This would increase the information available to consumers, assisting them to make an informed decision on where to take their business. As a result, businesses would be incentivised to increase investment into cyber security resources in order to differentiate themselves from competitors and attract clients or consumers.

### ***Promoting Participation***

A scalable system would also support a more rapid uptake of the health check program as it could encourage competition between businesses. However adoption of this style of health check program may prove more challenging for micro to medium businesses. The involvement of this business sector is crucial to the success of a health check program and a number of initiatives will need to be explored to capture an adequate level of engagement.



These smaller businesses will generally have a lower level of annual turnover and therefore allocate limited resources to cyber security. A 2020 survey by ACSC found that almost half of the small to medium business respondents invested less than \$500 on cyber security and only 20% spent between \$500 and \$999 on cyber security initiatives. The Commonwealth Government could facilitate increased participation from small to medium businesses through the use of a grant system. Another alternative could be to provide free access to subject matter experts from an organisation like ACSC if a smaller business is seeking to make an application for accreditation. This would support vulnerable businesses with the development and testing of Critical Incident Response plans as well as recovery from a cyber-incident.

While every effort should be made to improve overall cyber security standards across the Australian economy there will still be circumstances where cyber criminals adjust their strategy and continue to be successful. For this reason, it is critical that a multi-pronged approach is adopted.

## **CLEAR LEGAL REMEDIES FOR CONSUMERS**

### **Consultation Questions**

26. What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?
27. Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

Consumer Protection is a strong advocate for improved access to justice for all parties who experience loss or damages as a result of a cyber-incident. In principle, either of the proposed options for amendments to the Australian Consumer Law (ACL) or Privacy Act would be a step in the right direction.

Under the current legislative framework there are limited viable options for a victim to seek compensation. These include the Tort of Negligence and the general provisions of the ACL. However, these legal remedies are untested in Australian courts and present an expensive and complex process for consumers already experiencing significant distress and financial difficulties. Similarly, the complaints process with the Office of the Australian Information Commissioner (OAIC) does not provide an avenue for a consumer to recover damages, which is a principal area of concern for scam victims.

### ***Issues with Current Regulatory Framework***

It is the experience of Consumer Protection that victims of cyber-crime will have recently lost a substantial portion of their savings in the form of a deposit or payment for a house, car or renovation project. As such, these victims face strong financial challenges and may not be in a position to engage the services required to effectively enforce their rights under the existing framework.

Due to the technical nature of such disputes there would be a clear evidentiary burden placed on the victim to demonstrate that the cyber incident occurred on a third party's cyber infrastructure or as a result of action by the trader. This could require costly expert opinions from a Forensic Auditor or other qualified IT professional. In addition, victims may face difficulties in finding appropriate legal representation through commonly utilised services such as Community Legal Centres given the limited precedent in this area.

Consumer Protection submits that every effort should be made to address structural imbalances in instances of successful cyber-attacks that result in payment redirection scams. Some examples of how such an amendment could work include:

- placing the onus of proof on businesses to demonstrate that a cyber-incident is not a result of their action (or inaction);
- utilising an arbitration model to empower regulator(s) to investigate claims and issue orders to resolve disputes; and
- ensuring that point of fault in a cyber-incident in a legal dispute is proven to the burden of proof of the balance of probabilities and not beyond reasonable doubt.

### ***Amendments to Privacy Act or Australian Consumer Law***

The inclusion of a Tort of Privacy style mechanism into the *Privacy Act 1988* (Cth) has significant merit. The OAIC is an independent statutory body with significant experience handling issues of this nature. The implementation of such a mechanism could also coincide with the expansion of the Privacy Act to be applicable to businesses of all sizes. However, one downside of any inclusion under the Privacy Act would be the relative lack of awareness surrounding this legislation and associated regulators. As such, significant resources would need to be committed to promote brand awareness and establishment of new working relationships.

In contrast, if an ACL amendment was to be enacted this would utilise a well-established network of regulators at a Commonwealth, State and Territory level. ACCC and Australian Securities and Investment Commission (ASIC) would likely need to play a significant role in the establishment of this new model. It is Consumer Protection's understanding that ACCC will also be making a submission to this review. This submission will state that ACCC supports the establishment of an independent cyber security regulator. Consumer Protection is also supportive of that position.

Regardless of how the Commonwealth Government intends to implement such a mechanism it is clear that it needs to be structured in a way to limit or remove such financial and evidentiary burdens to ensure adequate access to remedies for even the most vulnerable of consumers or businesses.

## **OTHER POLICIES**

### **Consultation Questions**

28. What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights of consumers?



A consistent approach is required across jurisdictions and through overarching legislation that relates to cyber security issues. One such area that should be reviewed to complement any of the amendments proposed in the discussion paper is the e-payments code of practice.

ASIC recently held consultation on proposed amendments to the e-payments code which would explicitly exclude scams, such as those caused by a cyber-incident. This included changes to the definitions of 'mistaken internet payment' and 'unauthorised transactions'. Consumer Protection feels that these changes are a step in the wrong direction and reduce consumer's rights to recover monies lost as a result of a scam or cyber incident, effectively working against the core principles that this discussion paper aims to address.

Instead, Consumer Protection advocates for the inclusion within the e-payments code of a "no blame" model similar to that recently implemented in the United Kingdom (UK). This would create a fair system of redress available to both consumers and small businesses. This model considers a combination of the individual circumstances of the victim and the scam itself, ultimately weighing this against whether or not it was reasonable for the consumer to have protected themselves. If it was not reasonable, for example, if the consumer is from a vulnerable group, or the scam was highly sophisticated, the consumer should be able to recover the funds. Most importantly, if a customer has been the victim of a payment redirection scam, the financial provider should reimburse the customer from a fund contributed to by both the financial sector and government.

The review also outlined ASIC's proposal to require financial institutions to encourage further uptake of the PayID system in lieu of implementing a "confirmation of payee" service. Consumer Protection's view is that this will be of negligible benefit in protecting consumers against scams. It places responsibility for creating a PayID on the individual consumer, rather than the financial institutions taking any responsibility for making this happen. This has resulted in a somewhat sluggish uptake of the system. By contrast, the "confirmation of payee" system places the responsibility on the financial institutions to implement the required changes, which in Consumer Protection's view is where the responsibility should vest. It would also accord with what many consumers believe is happening at present – that financial institutions are matching the account name with the account number. It is worth noting that the software to make the comparison between the account name and account number is already available; it is currently being used in the UK. This "confirmation of payee" system would make an immediate positive impact in preventing payment redirection scams with minimal regulatory cost to financial institutions. It would not allow an environment that is rich for payment redirection scams to continue to thrive while the community waits for increased uptake of the PayID system.

The Commonwealth Government will need to carefully consider any changes to cyber security regulations and standards as a whole of Government issue. One Commonwealth Department or Commonwealth Regulator diminishing cyber security standards and redress options, while others strengthen them, will create inconsistency that will essentially undermine efforts to improve cyber security regulations as a whole.

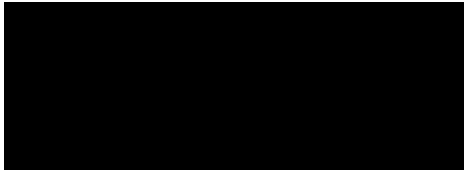
## CONCLUSION

Consumer Protection is supportive of the Commonwealth Government actively taking steps to address the issues of cyber-crime and related scams on the Australian economy. Consumer Protection's goal is for government and business at all levels to collaborate to effectively disrupt and deter cyber-crime in order to actively reduce its economic and psychological impact on both consumers and businesses.

We encourage the Department of Home Affairs to consider the suggestions outlined in our submission. Consumer Protection hopes to see changes that promote the improvement in the cyber security resilience of businesses as a whole and improve options for redress where there are occurrences of cyber incidents.

If you would like to discuss Consumer Protection's comments further, please contact Ms Patricia Blake, Director Retail and Services, on [REDACTED] or via email to [REDACTED].

Yours Sincerely



Gary Newcombe

**COMMISSIONER FOR CONSUMER PROTECTION**