AUSTRALIAN AUTOMOTIVE DEALER ASSOCIATION

Critical Infrastructure Reforms Team
Cyber and Infrastructure Security Centre
Department of Home Affairs

Date: 04 March 2024

A: PO Box 25, Belconnen ACT 2616
Submitted via email

2023–2030 Australian Cyber Security Strategy: Legislative Reforms

The Australian Automotive Dealer Association (AADA) welcomes the opportunity to submit a response to the 2023-2030 Australian Cyber Security Strategy: Legislative Reforms.

The AADA is the peak industry advocacy body exclusively representing Australia's 3,179 franchised new car Dealers. New car Dealers are predominantly privately- owned family businesses operating in cities, suburbs and regional towns across the country. The industry directly employs more than 61,000 people making a total economic contribution of over $18 billion.

The AADA's comments on the content of the consultation paper are in relation to franchised new car and truck Dealers, referring to the reporting matters canvassed in Measure 2 of the consultation paper.

Cyber-attacks and fraud can be a significant risk for franchised new car Dealers, through attacks that target a franchisor/supplier and as a result, prevent franchisees from using essential trading systems. Disruptive or permanent damage can be done to critical systems, for example, stock ordering, processing transactions, arranging finance, and communicating with customers can all be impacted.

Recent experience has shown that franchisee businesses are vulnerable when franchisor systems are compromised. For example, late in 2023, a vehicle manufacturer's systems were attacked, and as a result, the systems that the franchisor operated and managed were unavailable to franchisees and essential business processes were disrupted. Later it became apparent that disruptions had occurred across multiple areas, including financial services, direct debit arrangements, and Dealer email communications.

The disruption scenario described above is a possibility for all Dealers where their businesses are linked by systems and dependent on a trusted ecosystem provided by a franchisor. Franchisees and their customers have significant reliance on the systems provided by the franchisor, so any attack or failure is a threat to the franchised systems due to the dependency on the franchisor's system and can cause damage to business operations and reputations.

Therefore, in answering some of the questions raised in the consultation paper, we comment from the perspective of franchisees who in our view must be considered when assessing the impact of a cyber-attack on their franchisor that can have significant impacts on their business operations. Franchisees must be advised swiftly and accurately as to how the franchisee can immediately secure systems and provide an avenue for the ongoing ability to trade.

In the example mentioned above of the cyber-attack on the manufacturer, it was more than a month after the first news of the attack when consumers were advised that customer data had been accessed. While appreciating that investigation of a cyber-attack can take time it is imperative that franchisees are informed quickly and assisted to act to protect their businesses and customers.

Franchisees are often digitally dependent on systems provided and operated by their franchisor or by third parties endorsed by the franchisor. Some franchisors also dictate specific software that must be installed and used. This creates significant dependence for the franchisee on their franchisor in the event of a cyber-attack, and we consider this to create an obligation for the franchisor to provide quick and decisive communication to mitigate consequences. The timing of advice and quality of advice is paramount to franchisees.

The AADA recommends that there should be some regulation or guidance which ensures that where a franchisor experiences a cyber-attack, data breach, hack, demand, or security failure: all franchisees are immediately advised and provided with advice on how to best and safely manage the impact on their business. If there is no impact, the franchisees must still be advised of the attack on the franchisor systems and kept informed of how the issue is to be managed by the franchisor and of any developments as they occur.

Any likely or anticipated impact on the franchised business operations should be included by the franchisor during investigations and provide a clear path of communication directly with the franchisor that franchisees can use to obtain direct assistance. Franchisors that experience a cyber-attack on their systems should also be required to provide regular and meaningful updates regarding the resolution of the issues and any risks to franchisees.

We would be happy to meet with you to discuss our submission and participate in any further consultation. If you require further information or clarification in respect of any matters raised, please do not hesitate to contact me.

Yours Sincerely,

James Voortman
Chief Executive Officer
jvoortman@aada.asn.au
0452 535 696