**FOR IMMEDIATE RELEASE:** 21 August 2023

Eftsure Pty Ltd

Niek Dekker

[niekd@eftsure.com.au](mailto:niekd@eftsure.com.au)

61 450 617 311

**Don’t pass the buck: How effective financial controls can mitigate fraud**

*Financial losses are a major consequence of cyber scams, but finance leaders now have a new resource to help them upgrade processes and fortify their defences.*

**Sydney, NSW:** The Latitude Financial, Optus and Medibank cyber attacks impacted millions of Australians in the past 12 months have made it clear that bolstering cyber defenses is a business imperative in 2023.

According to the Australian Competition and Consumer Commission, the business community saw a total loss of $23.2 million, a 73 per cent increase from last year. However, this only accounts for some reporting data, meaning that actual numbers are likely larger.

“Lowering the risk of these scam losses requires a multi-faceted approach,” says Mark Chazan, Chief Executive Officer of Eftsure, a B2B payment protection solution that safeguards over $180 billion annually. “One part of that approach should be strengthening internal controls and ensuring that digital fraud prevention is built into finance processes.”

To help businesses strengthen those controls, Eftsure has released a comprehensive guide for finance leaders.

The Financial Controls Guide walks through a collaborative, multi-functional approach for assessing, upgrading and correcting an organisation’s financial processes. As owners of these processes, Chazan says that Chief Financial Officers (CFOs) are in the best position to drive stronger anti-fraud controls.

“To build a strong cyber defence, organisations need to evaluate their people, processes and technology.”

The guide will help CFOs zero in on the “processes” part of that equation, an important step in what Chazan refers to as “collaborative cybersecurity.” A collaborative approach is critical, says Chazan, because organisations aren’t fighting a fair fight.

“Scammers only need to be successful once, whether that’s getting an employee to click on a malicious link or impersonating a trusted contact. Conversely, organisations need to be successful at stopping these attempts *every* time – or else they could face serious financial, legal and reputational damage.”

This approach aligns with what is currently known about Australia’s new national Cyber Security Strategy. Minister for Home Affairs and Minister for Cyber Security, Claire O’Neil, has emphasized a collaborative approach to both developing and implementing the 2023-2030 Australian Cyber Security Strategy, which will outline the Government’s long-term vision for cybersecurity.

“It’s the step-change Australia needs to improve our national resilience to cyber threats and properly address the consequences of cyber incidents,” Minister O’Neil has said.

“We must work together to counter these threats, build partnerships and set ourselves up for success. Everyone has skin in the game when it comes to Australia’s cybersecurity.”

From a business perspective, implementing an effective financial controls strategy is a step towards bolstering the organisation's overall cyber security posture that will enable it to effectively protect sensitive company and customer data – keeping cybercriminals at bay while it is business as usual

**About Eftsure**

Eftsure is Australia's market leader in payment fraud prevention. Specifically designed for businesses, our end-to-end solution safeguards more than $180b in B2B payments per year. Our mission is to build a safer business community. With a large and continuously growing database of verified supplier details (the only one of its kind), we use multi-factor verification to give businesses greater knowledge and control over onboarding suppliers, receiving invoices and making payments. In short, we ensure our customers never pay the wrong people.

**Niek Dekker**

Head of Marketing

niekd@eftsure.com.au

61 450 617 311