eftsure Pty Ltd
ABN 21 168 403 736
ACN 168 403 736

Level 6, 122 Walker St,
North Sydney 2060
1300 985 976

eftsure.com.au

25 February 2022

Data Economy Unit
Consumer Data Right Division
The Treasury
By email: eInvoicing@treasury.gov.au

Dear Sir/Madam

Re: SUPPORTING BUSINESS ADOPTION OF ELECTRONIC INVOICING, Consultation Paper, December 2021

Eftsure welcomes the opportunity afforded by the Australian Treasury (Treasury) to provide feedback and comments into the adoption of electronic invoicing (eInvoicing).

ABOUT EFTSURE

Eftsure is a unique Australian fraudtech platform that ensures organisations can process Electronic Funds Transfer (EFT) payments securely, by mitigating the risk of fraud and error. Gaps in Authorised Deposit-Taking Institution (ADI) verification systems result in an Account Name not being matched against a BSB or Account Number when EFT payments are being processed.

This verification gap results in a range of heightened risks for Australian organisations:

External Risks:

Criminal syndicates, often based overseas, use a variety of tactics, such as Authorised Push Payment (APP) or Business Email Compromise (BEC) attacks, to engage in invoice fraud. This involves deceiving Accounts Payable (AP) staff into amending supplier payment details, resulting in funds being erroneously and irretrievably paid into bank accounts controlled by the criminals.

Such fraud ranks as the most common type of cybercrime according to the Australian Cyber Security Centre (ACSC). It represents 39.86% of all reported cybercrimes.[1] In FY 19-20, reports of BEC scams to the ACSC cost Australian organisations in excess of $142 million.[2]

Internal Risks:

Gaps in ADI verification systems can also result in malicious internal actors manipulating supplier payment data in Enterprise Resource Planning (ERP) systems or the text-based Australian Banking Association (ABA) files that are used to process EFT payments in online banking portals. These verification gaps can also increase an organisation's risk of incorrect payments due to human error. This typically occurs when AP staff incorrectly enter payment data manually.

Launched in 2016, the Eftsure platform helps mitigate these risks by enabling AP functions to cross-check their supplier banking records against an aggregated database comprising over 2.5 million Australian organisations. By verifying that the banking details being used to process EFT payments align with the details used by other organisations when paying the same supplier, organisations gain

[1] https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf
[2] https://www.cyber.gov.au/acsc/view-all-content/news/business-email-compromise

assurance that their supplier records are accurate. This reduces their exposure to financial losses resulting from fraud or error.

OVERVIEW

This consultation process is an opportunity to examine ways to advance the adoption of eInvoicing by Australian businesses. It focuses on two broad potential strategies:

1) Introducing a Business eInvoicing Right (BER)
2) Helping businesses integrate eInvoicing into their existing processes through:
    a. Fostering adoption of Peppol-compatible electronic data interchange (EDI) networks;
    b. Expanding eInvoicing into Procure-to-Pay processes; and
    c. Encouraging greater integration of payments and eInvoicing processes.

Given the rapid expansion of digital business-to-business (B2B) payments, as well as an exponential rise in invoice fraud stemming from the inherent security vulnerabilities that exist in current invoice delivery and handling practices, the Treasury's advocacy of eInvoicing is both needed and timely.

As an organisation committed to mitigating the risks associated with invoice fraud, Eftsure is a keen advocate of expanding the adoption of eInvoicing.

However, whilst the adoption of Peppol-compatible EDI networks, including the use of eInvoicing, will undoubtedly result in higher levels of security, it should not be viewed as a panacea that will eliminate all instances of invoice fraud.

Business adoption of eInvoicing

Consultation questions:

1) **Should a Business eInvoicing Right (BER) be introduced to accelerate business adoption of Peppol eInvoicing?**

The introduction of a BER would be an important first step in encouraging greater adoption of eInvoicing.

However, an extended transition time would be required as many organisations have developed customised EDI protocols that meet their specific requirements. Any moves to force organisations to adapt their existing systems to be compatible with an open standard such as Peppol will inevitably result in a range of technical and logistical challenges.

Introducing a BER without sufficient planning could result in downtime that delays invoicing and payments, producing the opposite outcome that eInvoicing seeks to achieve.

Other considerations when it comes to the introduction of eInvoicing is whether such systems will provide sufficient levels of security against hacking attempts. Attempts to interrupt, disable, defraud and corrupt eInvoicing systems, whether by criminal or state-based malicious actors, could result in widespread disruption, with significant impact on the broader Australian economy.

The introduction of a BER, and subsequent widespread adoption of eInvoicing technologies, would make eInvoicing an important component of Australia's financial ecosystem, itself deemed a critical national industry. As such, it is essential that strong controls be in place to protect the integrity of

eInvoicing systems. There must be strong mandated verification and vetting of all participants in such systems.

Expanding eInvoicing into Procure-to-Pay

Consultation questions:

18) **What are the key business considerations and impacts relevant to expanding from eInvoicing to a broader integrated P2P process (such as Peppol P2P)?**

An efficient and secure Procure-to-Pay (P2P) cycle is critical for any organisation.

Accounts Payable functions can quickly become overwhelmed when processing large numbers of invoices from hundreds, if not thousands, of suppliers. Rigorous controls throughout the P2P cycle help ensure that:

a) Legitimate invoices are paid correctly and in a timely manner;
b) Suppliers are verified for accuracy and compliance purposes; and
c) Losses due to fraudulent or erroneous payments are mitigated.

At present, most organisations implement a range of data-centric manual controls to secure their P2P processes. Data must be aligned both internally, between different departments within an organisation, and externally with suppliers' systems

For example, 3-way matching requires aligning both internal and external data. Invoice data from the supplier (external) must be matched against the Purchase Order from the requisitioner (internal) and the Receipt Note from the receiving department (internal).

By adopting consistent data standards, such as Peppol, throughout the P2P process, maintaining rigorous controls will be easier, resulting in greater efficiencies.

However, another key consideration for business when adopting Peppol, not only for use in eInvoicing, but throughout the entirety of their P2P processes, is how its adoption will interact with data coming from overseas. Whilst numerous countries, including many European states, Singapore, New Zealand, and others, are adopting Peppol, many others are not. It is important that whatever standard is adopted in Australia should be as interoperable as possible with other standards used overseas, so as not to create friction in P2P processes which could introduce unintended inefficiencies.

Integrating eInvoicing with payments

Consultation questions:

22) **Given the market is currently working to deliver solutions that enable integrated eInvoicing and payments, what (if any) further action or intervention is required to address any current barriers to greater integration and help drive this process?**

Integrating eInvoicing with payments has the potential to facilitate a significant increase in payments security. It is a trend that should be encouraged. However, it also demands caution, as sophisticated cyber-criminals will still identify opportunities to manipulate invoice data, even following the widespread adoption of eInvoicing.

Like all applications, those used in the facilitation of eInvoicing are not immune to vulnerabilities and breaches which could enable the manipulation of payment details, resulting in fraud. In fact, there is a heightened risk that should vulnerabilities be identified in any of the widely used eInvoicing software platforms, invoice data manipulation could be automated. Ironically, this may result in significantly higher instances of payment redirection fraud.

To ensure that businesses are able to derive the many efficiency benefits of eInvoicing, it is also essential to build in strong data verification controls, in particular payment data. Ideally, this would be achieved through a range of measures, including rigorous identity and compliance checks when suppliers are onboarded, as well as the continuous verification of supplier banking details through integrated APIs with collaborative solutions across both financial institutions and external specialist industry solutions.

It is important to recognise that cyber-criminals will always seek to identify security gaps and weaknesses for attack. By ensuring interoperability with industry participants that have specific domain expertise, the systems to identify weaknesses and the ability to verify the legitimacy of payment data, it will help mitigate and stop attempted subversion.

Such measures, when adopted in conjunction with eInvoicing, will enable businesses to efficiently process invoices, whilst simultaneously strengthening payments security and mitigating the risks of invoice fraud.

Eftsure thanks Treasury for this opportunity to contribute to this important consultation process into eInvoicing. Should Treasury wish to further explore any matters raised in this submission, Eftsure would be pleased to fully cooperate.

Yours sincerely

Mark Chazan
Chief Technology Officer
Eftsure Pty Ltd
Eftsure.com.au
1300 985 976