01 February 2021

Matthew Sedgwick

Submission to the Australian Government Department of Treasury

e-invoicing@treasury.gov.au

RE: ProvenDB Submission to the Australian Government Department of Treasury on the Options for mandatory adoption of electronic invoicing by businesses

Dear Matthew,

Thank you for the opportunity to write to the Australian Government Department of Treasury on the Options for mandatory adoption of electronic invoicing by businesses. In the submission below, we describe our technology to highlight our expertise at ProvenDB and describe how our technology category might play a role in an e-invoicing solution.

1 ProvenDB Technology Expertise

ProvenDB is a platform for trusted data storage that integrates traditional database technology with the integrity, tamper-resistance and provability of Blockchain technology.

ProvenDB allows you to:

- Prove ownership of intellectual property
- Prove timestamps for legal instruments
- Prove that database records have not been tampered with or falsified
- Create a log of all document changes

ProvenDB Compliance Vault is a cost-effective software solution built on the ProvenDB platform that provides a tamper-resistant digital store for critical compliance information. The ownership and creation date of information stored in ProvenDB Compliance Vault can be definitively proven by stringent industry-standard cryptography, backed by public Blockchain transactions.

2 E-invoicing vulnerabilities

E-invoicing finds itself in the media spotlight because of the vulnerabilities surrounding the integrity of invoices and the issue of "man in the middle" attacks. Both of these should be considered when evaluating the risk to organisations using e-invoicing and how these may lead to the business losing money, fines and reputational damage.

2.1 Invoice Integrity

Invoice integrity is an issue that organisations face due to ease with which digital information can be fabricated and manipulated. Digital tampering represents a vulnerability for organisations because privileged insiders are often able to change invoices records and supporting documents without leaving any digital trace. In the Royal Banking Commission, there were numerous accounts of file restructuring and doctoring by financial advisors to remove evidence of wrongdoing. Using an auditable system that tracks all changes to documents is essential to increase the level of trust an organisation has in its internal processes.

2.2 Man in the middle attack

The man in the middle attack (MITM) is a common attack that involves the attacker secretly relaying and possibly altering communication between parties who believe they are directly communicating with each other. In the context of e-invoicing, the MITM could be impersonating either the buyer or seller to manipulate bank details, invoice charges and even covering their tracks by deleting and forwarding email chains.

1.4 Dispute resolution

In the event of a dispute between two contradictory invoices that purport to represent a single transaction, it may be difficult or impossible to determine which version of the invoice represents the true and original transaction.

3 APRA's guidelines to support e-invoicing

We believe that following the APRA data risk guidelines can support the implementation and reduce the vulnerabilities of the e-invoicing initiative. We believe, these guidelines can only be fully realised by the use of distributed ledger or Blockchain technology. Specifically (our emphasis):

> *Auditability (the ability to **confirm the origin of data** and provide **transparency of all alterations**) is a key element to verifying data quality. It involves the examination of data and associated audit trail, data architecture and other supporting material. APRA envisages that a regulated entity would ensure that **data is sufficiently auditable** in order to satisfy the entity's business requirements (including regulatory and legal), facilitate independent audit, assist in **dispute resolution (including non-repudiation)** and **assist in the provision of forensic evidence** if required*[1]

These guidelines are broadly applicable across almost all regulatory contexts but are particularly relevant in the context of the e-invoicing initiative. Implementing the guidelines would benefit the initiative by promoting confidence and minimising risk for buyers and sellers. Existing solutions are subject to both insider falsification and external hacking. We would assert that the use of public Blockchain transactions to prove the integrity of e-invoices can ensure the absence of tampering and provide an ability to prove provenance and invoice origin.

4 Mitigation of e-invoicing risks

Given the current state of technology, there exist two broad solutions to the risks inherent in an e-invoicing mechanism:

1. A trusted third party serves as the witness to each transaction. Email service providers often unwittingly serve this role when email trails are used to try and attest to a transaction's veracity.
2. E-invoices are digitally signed (to prove "who") and digital signatures anchored to a public blockchain or trusted permissioned Distributed Ledger (proving the "when").

The witness paradigm – currently the most widespread practice – is fraught with vulnerabilities and indeed can be seen to be failing to provide an adequate level of trust and security in the existing landscape. "Trusted" third parties concentrate the risk within any system and become an obvious target for cyberattack. On the other hand, blockchain technology represents a technological solution that is highly resistant to cyber-attacks, requires no "trusted" third parties and provides immutable and demonstrable proof of transactional integrity.

We believe that digital signatures combined with blockchain anchors represent the best option for ensuring trust and tamper-proof digital communications and that any e-invoicing solution ought to consider a role for these technologies.

[1] https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk_1.pdf