CYBERSECURITY AND COMPETITION:

ENABLING A SAFER, STRONGER E-CONVEYANCING MARKET

30 APRIL 2025

SOFTWARE@SCALE

TABLE OF CONTENTS

SOFTWARE@SCALE

Executive Summary

This submission provides an independent industry perspective on the cybersecurity implications of opening Australia's e-Conveyancing market to multiple Electronic Lodgement Network Operators (ELNOs). It argues that competition, far from undermining system security, can strengthen resilience by encouraging innovation, reducing single-vendor monocultures, and broadening the pool of defenders.

Software@Scale is a specialised consultancy with over 90 highly skilled professionals delivering secure, scalable technology solutions for complex environments. Our team has deep experience across financial services, payments, and cybersecurity, including the delivery of critical infrastructure for major banks and government.

Drawing on proven Australian precedents, including the Consumer Data Right (CDR), Standard Business Reporting (SBR), and the NBN wholesale model, we illustrate how multi-party ecosystems can securely share data and coordinate incident response without vendor lock-in.

We identify six core cyber-risk themes in a competitive e-Conveyancing environment: (1) message integrity; (2) credential revocation; (3) breach containment; (4) weakest-link resilience; (5) attack-surface management; and (6) coordination and oversight. For each, we summarise how industry standards such as the ASD Essential Eight, APRA CPS 234, ISO 27001, and the forthcoming e-Conveyancing Payments Industry Code, already mandate robust controls.

We then propose a set of practical, action-oriented recommendations addressed to the appropriate governance bodies, State & Territory Registrars, and relevant agencies. These include mandating an annual industry security baseline; convening a cross industry Cyber Coordination Forum; extending Critical Infrastructure Directions to all ELNOs; embedding security requirements into licensing frameworks; updating Commonwealth PKI policy; and forming a federated Logging & Analytics Consortium.

Implementing these measures will preserve the cybersecurity of e-Conveyancing while unlocking the consumer, innovation, and resilience benefits of a competitive market.

Introduction

Electronic conveyancing is central to the transfer of land title and settlement of property transactions in Australia. Following its introduction in 2013, the e-Conveyancing ecosystem has grown around a single dominant ELNO, raising concerns about monopolistic behaviour and single point of failure risk. The Senate Economics References Committee inquiry into micro-competition opportunities presents a timely opportunity to examine how opening the market to multiple ELNOs affects cybersecurity.

This submission addresses only the security dimension. We set out why competition complements cyber-resilience, analyse key risk themes in a multi-operator system, draw on Australian case studies, and conclude with targeted recommendations. The goal is to demonstrate that given the right governance and standards a multi-ELNO market can meet and likely exceed the security of today's mono-operator model.

Why Competition Strengthens Cyber Resilience Innovation

Organisations innovate to differentiate through security features, user experience, and reliability. In monopolistic settings, incentives to invest plateau once a “good enough” security baseline is achieved. Conversely, competing ELNOs will pursue novel threat detection, faster patching, and improved automation to win and retain customers.

Technological Diversity as a Security Asset

Competition naturally drives ELNOs to adopt different technology stacks, deployment models, and cloud providers, which in turn breaks the “single-vendor monoculture” that can turn a single flaw into a systemic outage. In a monopolistic framework, a bug in one messaging gateway or misconfiguration of a shared library would threaten every transaction. In contrast, when multiple operators each select distinct middleware platforms, encryption libraries, and hosting environments, a vulnerability in one simply cannot leap to the others.

This principle is well proven in Australian financial services: APRA regulates banks operating on a variety of core banking systems (e.g. Temenos, Finastra, Oracle) with identical security controls, yet no major correlated breaches have occurred. Likewise, the SWIFT ISO 20022 migration saw dozens of vendor implementations interoperate securely and no single software defect ever rippled across the network. Competition thus underpins resilience by mandating uniform standards such as APRA CPS 234 and ASD ISM while allowing each ELNO to innovate. The ecosystem benefits from both rigorous security baselines and the protective effect of diversity.

Fault Domain Segmentation & Fail-Over Capacity

With multiple ELNOs operating in parallel, interoperability creates a baseline that can be extended to enable settlement time failover for transactions that are ready to settle. If one provider experiences a localised outage or degradation, those pending settlements can be redirected through an alternate gateway, ensuring continuity. This n+1 resilience model is already standard in Australian payments. Banks leverage both the RITS and SWIFT gpi networks so that if one rail is unavailable, critical funds transfers still proceed on the other.

Competitive Incentives for Third-Party Assurance

Monopolies often have little reason to subject themselves to rigorous external audits or bug-bounty programs beyond the regulatory minimum. In contrast, competing ELNOs can differentiate by pursuing higher tier certifications (SOC 2 Type II, ISO 27017 cloud controls, PCI DSS for payment legs), commissioning independent penetration tests, and running public bug bounties. This drives a perpetual “arms race” in assurance that lifts the entire market’s security floor.

Rapid Standard Adoption & Experimentation

When multiple vendors vie for business, they’re more willing to pilot cutting edge defences including behavioural analytics, UEBA (User and Entity Behavior Analytics) and AI-driven threat-hunting. This is because the cost of being first mover is offset by winning new customers.

Supply Chain Diversification

Just as technology stacks themselves are diversified, competition allows ELNOs to choose from multiple hardware, software, and cloud vendors. This fracturing of supply chains prevents a “single-supplier shock” (e.g. the 2021 Microsoft Exchange proxy logon vulnerability) from cascading across the entire industry. Financial regulators already mandate that banks avoid single points of external dependency and ELNO competition mirrors and extends that resilience model.

Knowledge Sharing

When an incident occurs at one provider, public-private and cross-industry forums facilitate rapid dissemination of Indicators of Compromise (IOCs) and best practices, raising the security posture of all participants.

Australian Proven Case Studies

Consumer Data Right (CDR)

The Consumer Data Right (CDR) was introduced in Australia via the Competition and Consumer Amendment (Consumer Data Right) Act 2019, with the initial “Open Banking” phase commencing in July 2020. The regime gives consumers the explicit right to port their banking data including transaction histories, product and service information, to accredited third-party providers (Accredited Data Recipients, or ADRs).

Today, CDR handles over 15 million API calls per month across 40+ banks and 150+ ADRs. Despite concerns that real-time accreditation checks or complex cryptography might bottleneck performance, average API latency remains below 200 ms on par with conventional banking APIs.

Since launch, there have been no confirmed cases of an ADR impersonating another, nor any bank accidentally leaking data to an unaccredited party. The combination of rigorous cryptography, certificate-based trust, and live revocation checks has proven robust at scale.

Standard Business Reporting (SBR)

SBR’s central gateway allows over fifty accounting and reporting platforms (e.g. MYOB, Xero, SAP and proprietary vendors) to submit financial and tax data directly to the Australian Taxation Office. Despite this scale, SBR has never suffered a cross-vendor data leak or tampering incident. Its architecture enforces per-vendor sandbox isolation, Web Application Firewalls (WAF) with schema validation at the edge, and a shared Security Information and Event Management (SIEM) that aggregates logs across all tenancies. This combination of logical separation and collective monitoring demonstrates that multi-tenant aggregation can be both highly efficient and inherently secure.

NBN Wholesale Retail Model

Under Australia’s NBN wholesale–retail model, NBN Co operates as a government-owned wholesaler that builds, maintains and upgrades the underlying fixed-line, wireless and satellite infrastructure, then offers standardised virtual circuits to any Retail Service Provider (RSP) on identical commercial and technical terms. Each

RSP's traffic is carried over VLAN-tagged Ethernet Virtual Circuits atop the shared physical network, ensuring cryptographic and logical isolation at Layer 2 and above.

All participants must adhere to ISO 27001-derived security requirements and the ASD Essential Eight. This is covering patch management, network segmentation, intrusion detection and incident-response protocols as mandated by the Telecommunications Sector Security Reforms and the ACCC's Wholesale Broadband Agreement. RSPs connect to NBN Co's operational and business support systems via mutually authenticated VPNs and API gateways, using X.509 certificates and OAuth tokens issued and revoked through NBN Co's central PKI and OCSP responder pool.

When outages or security events occur, NBN Co convenes all affected RSPs in a central Operations Incident Room and publishes real-time updates on its Service Status Dashboard, then leads post-incident "Lessons Learned" sessions through the NBN Co–RSP Technical Forum to share root-cause analyses and remediation plans across the ecosystem. Since its 2011 launch, there has never been a breach in which a misconfiguration or vulnerability at one RSP compromised another's service, demonstrating that rigorous standards, logical isolation and coordinated governance can support a competitive, multi-retailer environment without increasing systemic risk.

Securing Competition - Threats and Controls

Opening e-Conveyancing to multiple competing operators need not dilute security, on the contrary, it unlocks a virtuous cycle of innovation, resilience, and shared learning. Australian multi-vendor programs have proven these key controls at national scale, showing that with the right guardrails, competition becomes the foundation of stronger, more adaptive cybersecurity.

The following controls require consideration regardless of whether there is one or many ELNOs.

Cryptographic Assurance at Every Hop

At the heart of any distributed ecosystem lies the need to verify that each message truly originates from who it claims. By mandating mutual TLS (TLS 1.2+ with strict certificate pinning, as prescribed in the ASD Information Security Manual) *and* end-to-end JSON Web Signatures on each payload (RFC 7515), every gateway and API call carries two independent proofs of authenticity. This "double envelope" approach underpins the Consumer Data Right (Case Study 5.1: CDR), where over a hundred banks and all accredited data recipients exchange millions of API calls weekly, and not a single spoofing incident has ever been reported. In e-Conveyancing, the same cryptographic rigor ensures that only a valid private-key holder can initiate or modify a transaction, neutralising any fear of message tampering even when multiple ELNOs interoperate.

Real-Time Credential Revocation

In any fast moving network, stolen or compromised credentials must be rendered useless in seconds. By issuing short-lived certificates or OAuth proof-of-possession tokens with lifespans capped at one hour and stapling each TLS handshake with a fresh OCSP response (per the Digital Transformation Agency's PKI Policy). The

moment an operator's accreditation is rescinded in the central CDR registry (Case Study 5.1), all subsequent calls are rejected automatically. Australia's Reserve Bank Information and Transfer System (RITS) applies this exact pattern to its high-value payment platform, guaranteeing that revoked participants cannot slip through during the next handshake. Applied to e-Conveyancing, federating these revocation feeds under governance oversight ensures that any subscriber who loses authority is instantly frozen out of the system.

Isolation & Containment by Design

Because each ELNO is a completely independent business with its own systems and keys, a security failure at one provider doesn't automatically give attackers a backdoor into another. Think of each operator as locked in its own steel vault room: even though they all sit in the same building, one vault breach doesn't open the others.

The key is to enforce that separation by enforceable rules, not assumption. Every ELNO must keep customer data under its own lock and key using unique encryption keys and strong network security and infrastructure controls so that even if they share the same cloud platform, their data never mingles.

The Standard Business Reporting scheme onboards over fifty accounting vendors into a single gateway, yet strict sandbox boundaries, application whitelisting, and tenant specific encryption have prevented any cross vendor data leak or tampering since 2004.

By embedding these simple principles into e-Conveyancing rules where each operator with its own isolated environment and keys we ensure that every ELNO stands alone and a breach at one cannot spill into another.

A Uniform Security Baseline

Diversity of platforms only strengthens resilience if everyone shares a common floor of controls. Mandating that every ELNO comply with standards and guidelines like ASD Essential Eight, ISO 27001, and APRA CPS 234, regardless of size, stack, or cloud provider ensures a level playing field. APRA's regime already applies this principle to dozens of banks running disparate core banking systems (Temenos, Finastra, Oracle, etc.), yet records no correlated breaches because each operator meets the same rigorous vulnerability management, encryption, and access-control requirements. e-Conveyancing should mirror this by embedding uniform controls into the Model Operating Requirements allowing regulators to ensure that no weak link can undermine the ecosystem.

Attack Surface Hardening

Every added gateway expands the potential surface for attack, but this can be tamed through centrally managed edge defenses and supply chain vetting. Following the Australian Government's Cloud Security Guidance, all public-facing APIs sit behind a unified Web Application Firewall with DDoS-scrubbing services, and undergo continuous automated vulnerability scanning. The NBN wholesale retail interconnect (Case Study 5.3: NBN) uses identical DDoS protection, rate-limiting, and geo-IP filtering at each peering point and has never suffered a systemic outage traceable to a gateway compromise. By replicating these same perimeter defenses for every ELNO

interconnect, e-Conveyancing can safely scale its multi-operator model without expanding risk.

Shared Governance & Visibility

Real-time visibility across operators is the cornerstone of coordinated incident response. Under the CDR program, the Data61-operated Sandbox Operations Centre aggregates logs, issues public Incident Bulletins within minutes, and convenes all Accredited Data Recipients in a “war room” to diagnose and remediate outages. A central Security Information and Event Management (SIEM) ingests telemetry from every participant (application logs, API traces, network flow data) enabling cross vendor analytics and early detection of fraud or tampering.

By standing up a forum led by an appropriate governance body across the relevant industry actors, you get all the benefits of a single playbook without a single vendor.

Through governance led “Lessons Learned” workshops and binding Service Level Agreements, every operator follows a common “Transaction Failure Playbook,” so that even complex multi-ELNO incidents are resolved swiftly and uniformly.

Recommendations

A resilient, interoperable e-conveyancing ecosystem doesn't require reinventing the wheel, just extending the proven safeguards that already secure Australia's most critical digital services. The same risk based frameworks (ASD Essential Eight, APRA CPS 234, ISO 27001 and ARNECC's Model Operating Requirements) that underpin banking, health data sharing and tax reporting can be applied across all ELNOs whether there is one or many. Similarly, joint incident response exercises, timely breach notifications, dynamic credential management and shared telemetry are standard practice in schemes like the Consumer Data Right and Standard Business Reporting. Embedding these governance driven, standards-based controls into e-conveyancing's interoperability layer will preserve security, simplify oversight and unlock the full benefits of multiple operators without introducing undue complexity.

Below are governance and standards recommendations to further support interoperability in the e-conveyancing ecosystem:

1. Embed Cryptography Standards
Introduce a standardised approach to mutual authentication and payload signing across ELNOs, governed by the appropriate bodies. This provides strong protection against tampering or spoofing with minimal operational overhead. Even one ELNO benefits by reducing risk from insider threats or compromised suppliers.

2. Strong Credential Management
Enforce time limited credentials and accreditation revocation managed through a governance body. This keeps revoked or compromised keys from being used and ensures only authorised participants can transact.

3. Best Practice Architecture - Isolation and Containment
Monitor best practice system separation and key isolation by an industry body, limiting the impact of any breach. Even for one ELNO, internal segmentation helps prevent lateral movement and keeps incidents controlled.

4. Industry Security Baselines
Set and publish a lightweight annual baseline aligned with existing standards like ASD Essential Eight and ISO 27001, governed by the appropriate bodies. This ensures a consistent security floor and helps operators avoid underinvesting, even in single vendor environments.

5. Protect the Perimeter
Require public interfaces to be protected by standard defences and regular checks. This keeps the system resilient to common internet threats and is straightforward to adopt using existing tools and practices.

6. Shared Governance and Visibility
Create a Cyber Coordination Forum containing the right representatives from operators and governance bodies to run joint drills, share anonymised insights, and issue alerts. This improves system wide awareness and response, even if there's only one operator involved.

SOFTWARE@SCALE

APPENDIX

SOFTWARE@SCALE

About Software@Scale

Software@Scale is a specialised consultancy with over 90 highly skilled professionals delivering high performance technology solutions for scalable and secure platforms. Our mission is to align technology strategies with business objectives, driving innovation, operational efficiency, and sustainable growth for our clients.

We have a proven track record delivering complex projects for major financial services organisations, with deep expertise in payment systems, cybersecurity standards, enterprise scale platforms, and regulatory compliance. We are known for navigating complex ecosystems with speed and precision, combining our ability to scale rapidly with a strong focus on high quality engineering outcomes.

Our team's credentials reflect our deep financial services and security pedigree:

- 45% of our engineers operate at Principal Level, specialising in complex, high volume platforms
- 55% of our staff are subject matter experts in banking, payments, and financial services ecosystems
- 30% of our engineers specialise in cloud infrastructure across Azure, AWS, and Google Cloud
- Our executive leadership team includes six former Commonwealth Bank of Australia (CBA) senior technologists and executives, all with extensive banking and payments expertise
- 75% of our staff have direct experience across banking, payments, insurance, and superannuation

Relevant Experience

Software@Scale is recognised for its deep expertise in delivering secure and scalable solutions for the financial services sector. Our people were instrumental in building critical platforms such as CBA's Netbank and Mobile App (digital banking), CommSee (branch CRM), and Commbiz (business banking). We have hands on understanding of the architectural decisions, intricate code dependencies, and enterprise wide integrations that underpin these platforms.

Our engineers have also played key roles outside of CBA, delivering secure financial platforms for Westpac, Fidelity Investments, Colonial First State, Recreo Financial, Team Super and Zip. These projects have included customer banking applications supporting millions of users, secure payment systems, core banking transformations, and high volume, high availability environments where security, performance and compliance are critical.

Security Expertise

Software@Scale provides specialist expertise across enterprise security architecture, cloud security, application security, data protection, DevSecOps, identity and access

management, threat management, automated vulnerability management, and darkweb monitoring and assessment.

Our security architects have designed and implemented enterprise grade security solutions across banking, insurance, media, and government, including leading programs for organisations such as the Department of Defence, CBA, IAG and QBE.

We have successfully led large scale security uplift programs, introduced secure-by-design frameworks, and driven initiatives aligned to NIST Cybersecurity Framework and ISO 27001 standards. Our team has also delivered critical infrastructure projects including secure AWS zoning models, vulnerability management platforms, DMZ architectures in cloud environments, and the deployment of next-generation security tooling across enterprise networks.

Our practical security experience supports the delivery of resilient, compliant, and high assurance platforms for financial services clients.

Depth of Capability

At Software@Scale, our technical strength reflects both the scale of projects we have delivered and the complexity of environments in which we operate. We have experience working across mission critical banking platforms, payments ecosystems, core financial services systems, and high availability cloud environments. Our teams combine strong technical skills with a detailed understanding of financial services standards, regulatory frameworks and operational obligations. Our proven experience allows us to deliver secure, scalable high performing solutions with confidence and precision.

- ***Extensive Financial Services Delivery***: Experience across CBA, Westpac, Fidelity Investments, Colonial First State, Recreo Financial, Fiserv, and Zip, spanning online banking, payments, insurance, superannuation, and consumer finance platforms
- ***Deep Payments and Security Expertise***: Delivery of secure, high volume payment systems, performance engineering for critical customer banking portals, and integration of observability and monitoring platforms.
- ***Innovative Engineering Leadership***: Our team helped define CBA's engineering frameworks for Specialist, Principal, and Chief Engineering roles, ensuring a disciplined and consistently high standard of engineering excellence. Software@Scale continues to actively uphold these standards of excellence.
- ***Proven Delivery Track Record***: Our specialists bring an average of six years' tenure at major banks and payments institutions, with over 90 years of collective delivery experience across Australia's largest financial services organisations

Software@Scale partners with financial services organisations to deliver secure, scalable, and resilient technology platforms that support innovation, compliance, and operational excellence.

Supporting Evidence

Australian Precedents

- **Consumer Data Right (CDR):** Multi-provider ecosystem managing highly sensitive financial data across dozens of banks and data holders without systemic breaches.
- **NBN Wholesale Model:** Diverse RSPs connect to a single infrastructure without monopoly; cybersecurity managed through uniform standards.
- **Standard Business Reporting (SBR):** Secure, multi-agency interoperability using federated trust frameworks.

Global Case Studies

- **SWIFT ISO 20022 Migration:** Dozens of banks, different vendors, same protocols — no correlated cyber failures.
- **US Financial Sector:** Competing banks running distinct systems under uniform FFIEC cybersecurity rules; promotes overall system resilience.

References

Australian Cyber Security Centre, “Essential Eight Maturity Model,” 2024. Available at: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

Digital Transformation Agency, “Cloud Security Guidance,” May 2023. Available at: https://www.dta.gov.au/standard/cloud-security-guidance

Australian Signals Directorate, “Information Security Manual (ISM),” 2024. Available at: https://www.cyber.gov.au/acsc/view-all-content/ism

Australian Prudential Regulation Authority, “Prudential Standard CPS 231 Outsourcing” and “Prudential Standard CPS 234 Information Security,” October 2021. Available at:

- CPS 231: https://www.apra.gov.au/sites/default/files/CPS 231_October 2021.pdf
- CPS 234: https://www.apra.gov.au/sites/default/files/CPS 234_October 2021.pdf

Australian Registrars’ National Electronic Conveyancing Council, “Model Operating Requirements,” June 2024. Available at: https://www.arnecc.gov.au/regulation/model-operating-requirements/

Consumer Data Standards Body, “Consumer Data Right Rules,” 2024. Available at: https://consumerdatastandards.gov.au/guidelines/rules

National Electronic Conveyancing Data Standards Ltd, “Interoperability Guidelines,” February 2025. Available at: https://www.necds.com.au/interoperability-guidelines

Standards Australia/ISO, “ISO 27001:2022 Information security, cybersecurity and privacy protection requirements,” 2022. Available at: https://www.iso.org/standard/82875.html