MUFG

MUFG Retirement Solutions
A division of MUFG Pension & Market Services

Protecting Australia's retirement savings in a digital world

How super funds can strengthen member protection with stronger security and smarter identity solutions.

Content

Introduction

The Australian superannuation industry, a key pillar of financial security for millions, is increasingly under siege from sophisticated cyber threats. The trust-based nature of the relationship between funds and their members, coupled with the vast sums of money under management, makes the sector an attractive target for malicious actors.

Recent cyber incidents, both within superannuation and across other critical sectors, highlight the need for enhanced protective measures and streamlined, secure processes. These incidents also emphasise the significant operational friction and member frustration caused by current, often manual, verification methods, particularly during times of crisis.

Reflecting on these concerns, APRA's June 2025 directive to RSE licensee boards highlights the urgent need to strengthen authentication controls under CPS 234, particularly for high-risk member activities and privileged access.

This whitepaper addresses these pressing challenges by exploring the evolving cyber landscape, drawing critical lessons from a recent significant cyber and market disruption event experienced by the superannuation industry. We detail our proactive response and the effectiveness of our security measures. Furthermore, we argue that while robust cybersecurity frameworks are essential, the strategic adoption of digital identity solutions represents the next crucial step.

Aligned to regulatory and consumer expectations, these solutions will strengthen member protection and improve the overall member experience by enhancing the speed and security of verification at every touchpoint in their superannuation journey. Thus, achieving a superior member experience and a more secure route for completion of updates and payments to members.

To help inform this view, MUFG Retirement Solutions commissioned a national research project* examining how Australians perceive and engage with digital identity in the context of superannuation, revealing key behavioural patterns, trust signals, and expectations for future verification journeys.

Australians are already familiar with digital identity tools – 69% regularly use facial recognition, fingerprint scanning, or document uploads in other interactions – indicating a strong foundation for adoption in superannuation.

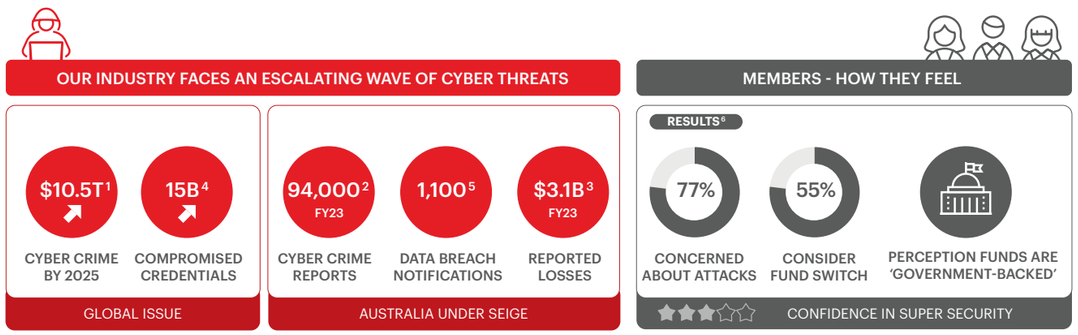
* In partnership with Askable Pty Ltd, MUFG Retirement Solutions' two-phase Digital ID research project was conducted in July 2025 with over 500 Australians. The project included in-depth qualitative interviews and a nationally representative quantitative survey to explore consumer attitudes, behaviours and expectations around cybersecurity and digital identity.

Executive Summary

The Australian superannuation industry faces an escalating wave of cyber threats, as evidenced by recent high-profile incidents and a significant increase in cybercrime reports. A shift to stronger protections and smarter digital identity solutions is crucial to protecting member assets and improving their experience.

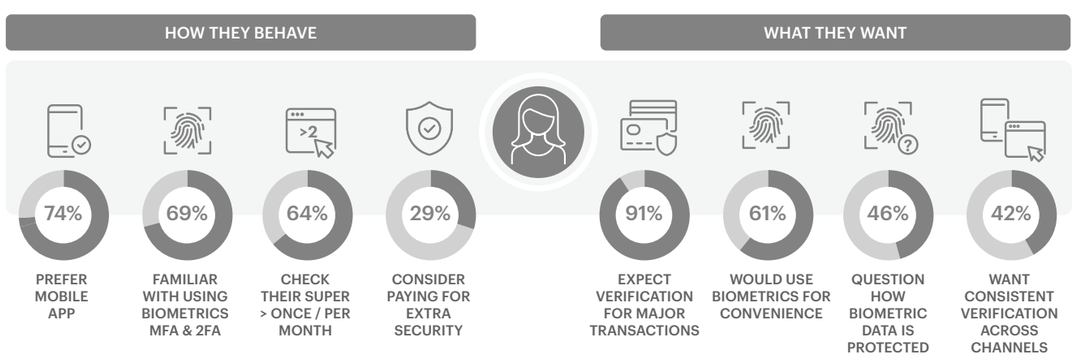
The argument for stronger protections

Cybercrime is a booming global industry, projected to hit $10.5 trillion[1] annually in 2025. Australia is not immune, with cybercrime continuing to escalate. In FY2022–23, the Australian Signals Directorate (ASD) received nearly 94,000[2] cybercrime reports - a 23% year-on-year increase - while the Australian Competition and Consumer Commission (ACCC) reported over $3.1 billion[3] in scam-related losses during the same period. The superannuation sector is a prime target.



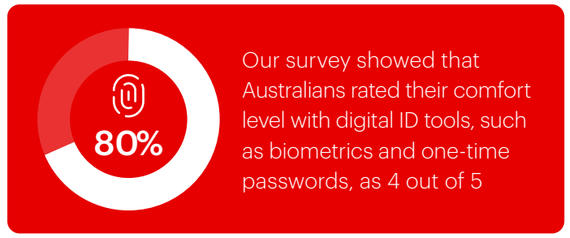
Understanding consumer behaviour and expectations

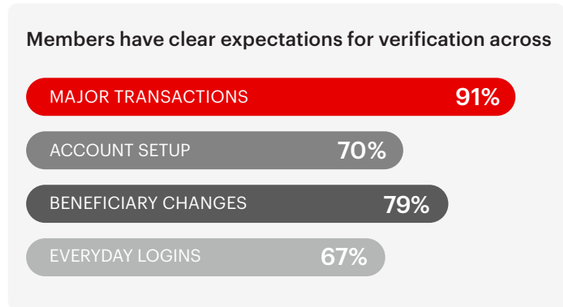
Our two-phase national research project[6], conducted in July 2025 in partnership with Askable Pty Ltd, involved in-depth qualitative interviews and a nationally representative survey of over 500 Australians. This research directly substantiates the need for change, uncovering key insights into everyday Australians' attitudes, behaviours and expectations around cybersecurity and digital identity.



Lessons from Disruption: A significant cyber and market event in Australia in April 2025 caused an unprecedented surge in member inquiries and technical issues. MUFG Retirement Solutions effectively managed this with its proprietary Analytical Link Exception Reporting Tool (ALERT), protecting an estimated $21 million in member funds in two months.

United Industry Front: The superannuation industry must present a united and collaborative front against evolving cyber threats. Sharing threat intelligence and collectively upholding robust security standards is crucial to minimise risks and maintain public trust.





Regulatory Imperative: APRA's June 2025 directive to RSE licensee boards reinforces the urgent need to re-assess and uplift of authentication controls under CPS 234, specifically following recent credential stuffing attacks. This regulatory action highlights areas for improvement and emphasises the importance of enhanced cyber defences to safeguard member funds and data.

Digital Identity is Essential: These solutions offer a dual benefit – strengthening fraud protection and streamlining member interactions. Australian businesses using identity verification technologies have already seen an 82% reduction in fraud and saved an average of $12 million[7].

Future of Identity: The proposed Trust Exchange (TEx) initiative, based on verifiable credentials, directly addresses APRA's call for stronger, fit-for-purpose authentication, especially where traditional MFA may fall short. The industry should actively support and participate in TEx's development to ensure it meets superannuation needs.

Considerations for Adoption: Funds must assess critical operational and strategic priorities for successful adoption, including technical integration, regulatory compliance, staff training and accessibility. Educating members on the benefits is crucial for trust and a smooth transition.

Commitment to Innovation: MUFG Retirement Solutions is proactively developing digital identity technology, partnering with Verified Orchestration to innovate and engage with government initiatives. This commitment aligns directly with APRA's regulatory imperatives, aiming to close authentication control gaps and advance the superannuation industry to protect the retirement savings of all Australians.

1. Cybersecurity Ventures, 2025 Official Cybercrime Report
2. Australian Signals Directorate, Annual Cyber Threat Report for FY2023–24
3. ACCC Scamwatch (2023). Scamwatch Report 2023
4. Digital Shadows. Dark Web Intelligence
5. Office of the Australian Information Commissioner (OAIC). February 2025
6. MUFG Retirement Solutions. Digital ID Research Report 2025
7. Docusign / Entrust Report cited by CFOtech Australia, April 2025

The cyber threat landscape

Cybercrime is a rapidly expanding global threat, with its financial and operational impacts growing exponentially.

15 billion compromised credentials are actively circulating on the dark web[2]

Global landscape

Cybercrime costs: Expected to cost the world $10.5 trillion annually by 2025, a dramatic increase from $3 trillion in 2015[1]. This highlights the escalating financial burden on businesses and individuals worldwide.

Credential stuffing: Over 15 billion compromised credentials are actively circulating on the dark web[2]. This vast repository fuels attacks like credential stuffing, where threat actors attempt to use stolen username and password combinations to gain unauthorised access to accounts on other platforms.

Financial impact: The average cost of a data breach globally reached USD $4.45 million in 2023[3]. These costs encompass incident response, lost business, reputational damage, and regulatory fines.

Top threats: Phishing, ransomware, and credential reuse attacks remain the most prevalent and effective attack vectors globally, continuously evolving in sophistication.

Australian context

The Australian landscape mirrors global trends, with specific challenges for local organisations.

Cybercrime reports: The Australian Signals Directorate (ASD) reported nearly 94,000[4] cybercrime incidents in FY2022-23, representing a significant 23% year-on-year increase. This surge indicates a heightened threat level for Australian entities.

Losses: Total reported losses from scams and cybercrime in Australia exceeded $3.1 billion[5], with Business Email Compromise (BEC) and investment scams leading the financial impact.

Identity crime itself is a significant issue. The Australian Institute of Criminology reported in July 2023 that 31% of Australians have experienced identity crime in their lifetime, with 20% experiencing it in the past 12 months. This threat demonstrates the financial and personal harm inflicted on individuals and businesses.

Time to detect: On average, Australian organisations take 33 days to detect and contain a cyber incident[6]. This prolonged detection period can exacerbate the impact of a breach, allowing threat actors more time to operate within compromised systems.

Financial services: The superannuation industry is a growing target. This vulnerability stems from the large sums of money held, the critical nature of retirement savings, and the inherent trust-based relationship between funds and their members, making it a prime target for identity theft and financial fraud.

These factors highlight the critical need for robust, multi-layered cybersecurity defences and proactive strategies within the Australian superannuation industry.

1. Cybersecurity Ventures. (2022). Cybercrime Magazine Q3 2022
2. Digital Shadows. (Ongoing research). Dark Web Intelligence
3. IBM. (2023). Cost of a Data Breach Report 2023
4. Australian Signals Directorate, Annual Cyber Threat Report for FY2023–24
5. ACCC Scamwatch (2023). Scamwatch Report 2023
6. Office of the Australian Information Commissioner (OAIC). (February 2025)

Learnings from cyber & market disruption

Overview of incident

On 4 April 2025, the Australian superannuation industry experienced a significant cybersecurity threat that was closely followed by the global stock market turmoil stemming from US trade policy changes.

Alongside superannuation funds and other providers, MUFG Retirement Solutions observed a substantial increase in credential stuffing activity targeting member accounts. This media-covered event, combined with global market volatility (US stock indexes saw their biggest daily percentage drops since 2020[1], and the Australian market fell nearly 3% on 4 April 2025[2]), led to an unprecedented surge in member enquiries and transactions.

The increased legitimate traffic, rather than malicious activity, caused intermittent performance issues across multiple systems, including our member and contact centre portals. Similar issues were reported by other superannuation funds and providers, with MUFG Retirement Solutions increasing our digital servicing capacity up to 700% to accommodate the increased requests from online members.

MUFG Retirement Solutions' quick response, proactive risk mitigation strategies, and extensive experience in managing similar events enabled us to effectively navigate this crisis. Our reporting controls allowed us to detect an increase in activity a few days prior to the event. While it is not generally unusual to observe indicators of threat activity in parts of our environment, as a precautionary measure, we immediately implemented heightened monitoring to respond to any potential threats. Our robust security controls proved effective, ensuring that member data and funds remained secure.

Member protection through ALERT

Actively protecting member data and assets since 2019, the ALERT system is MUFG Pension & Market Services' proprietary monitoring system, and the only one of its kind tailored to the superannuation industry.

This highly sophisticated platform delivers real-time protection at scale by analysing hundreds of millions of data points daily. Leveraging advanced analytics, law enforcement intelligence, and a constantly evolving library of cybersecurity vulnerabilities, ALERT identifies suspicious activity and prevents significant losses across a wide range of cyberattack and external fraud risks.

By integrating these data streams, ALERT's Robotic Process Automation (RPA) significantly accelerates protection at scale. Currently monitoring over 30 million accounts, ALERT processes approximately 450 million data points daily. During the most recent event, it triggered the investigation of between 5,000 to 10,000 accounts per day, ultimately protecting an estimated $21 million in member funds over a 2-month period.

30 million
accounts monitored daily

450 million
data points analysed daily by ALERT

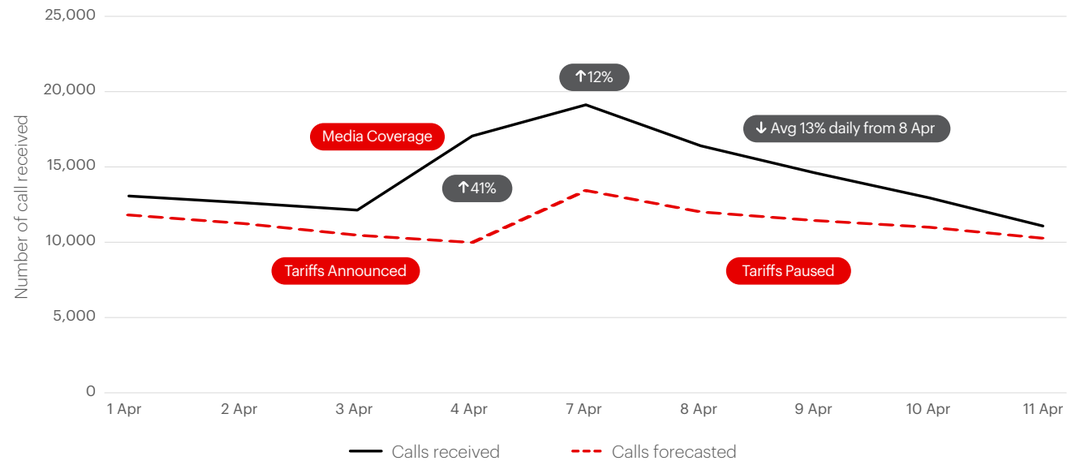
$21 million
protected over 2 months

5k-10k
accounts investigated

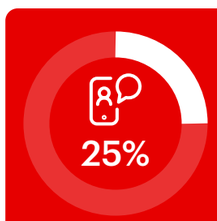
1. reuters.com
2. abc.net.au

Member interaction insights

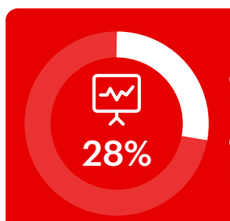
The surge in member enquiries following media coverage and market volatility presented significant operational challenges.



- Call volumes increased by 41% on 4 April following media coverage, peaking at 71% above forecasted volumes. A further 12% increase was observed on 7 April
- Clear communication on protection measures and the 9 April pause on reciprocal tariffs contributed to a 13% average day-on-day reduction in call volumes
- 28% of calls were related to investment performance concerns driven by market volatility
- 25% of calls were from members seeking information about the cyber threat, including concerns around security, fraud, and account safety



Calls were from members seeking information about the cyber threat, including concerns around security, fraud, and account safety



Calls were related to investment performance concerns driven by market volatility

Operational resilience & proactive management

The incident invoked immediate attention from our Crisis Management Team (CMT), along with frontline Services and Operations areas. Consistent and transparent communication with regulators, funds, and members was critical as industry activity intensified. This event was a critical learning for the industry and a demonstration of our operational resilience.

During the peak of the April 2025 disruption, we successfully monitored over 30 million accounts and investigated up to 10,000 suspicious accounts in real time. We were able to quickly scale our technology and systems, manage heightened call volumes, deploy active queue management, and extend operating hours to effectively support our clients and their members through this high traffic period in a safe and secure manner. This experience highlights the investments we've made in infrastructure, systems and processes to strengthen our resilience under extraordinary market and cyber conditions.

Surge in calls and transactions

- Call volumes increased by 41% on 4 April 2025 and peaked at 71% above forecasted volumes.
- Administration work on hand rose by 26% in the week commencing 7 April 2025, particularly in benefit withdrawal requests, emails, and investment enquiries.
- Member investment changes increased by an average of 320% compared to the previous week.

Extended hours, scaling to meet demand

- In consultation with funds, contact centres operated over two weekends to cater for increased call volumes.
- Workforce plans were executed to deploy resources and maintain critical services outside standard operating hours.
- Appropriately skilled resources were actively redirected to high-volume administration activities, leveraging our scale and depth of capability.

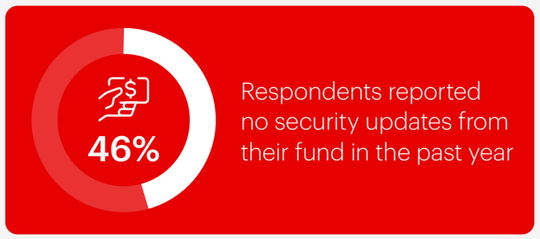
Partnering with funds for member assurance

- We collaborated closely with funds to ensure website and portal messaging effectively addressed member concerns.
- Direct email communications were sent to members to ease concerns about market volatility and cyber threats.
- Fund-approved telephony-based messaging (IVR) was deployed to provide immediate information and guidance to callers.

Survey participants reported they had moderate to high concern about cyber threats

Notably, even before this event, 77% of Australians we surveyed already reported moderate to high concern about cyber threats.

This heightened sensitivity further explains the surge in member contact during incidents and supports the need for clear, proactive security communication.



Respondents reported no security updates from their fund in the past year

46% of those surveyed did not recall receiving a security update from their fund in the past year.

The incident highlighted the relationship between cybersecurity threats, market events, and member behaviour, emphasising the importance of strong operational resilience and proactive crisis management in the superannuation industry.

Insights for a united superannuation industry

Learnings from recent events should be leveraged to establish a consistent, industry-wide approach to cybersecurity and ensure a united front in future crises.

Information security leaders network: We believe there is benefit in the superannuation industry establishing a Chief Information Security Officer (CISO) community. This network would meet regularly to share experiences, exchange threat intelligence, and collectively minimise risks across the broader industry. Security must be managed as a united front, taking cues from the banking sector's successful collaborative models.

One voice for the industry: It is also critical to have one clear, consistent, and authoritative voice for the industry during such incidents to maintain public trust and prevent unnecessary panic. MUFG Retirement Solutions would be highly supportive of leading such a community for the benefit of the broader industry.

Member portal access & MFA: We strongly recommend deploying Multi-Factor Authentication (MFA) across all member portals and mobile apps to maximise security. This aligns with APRA's guidance to trustees, which reinforces the obligation to implement authentication controls that reflect the sensitivity of member data.

Where MFA is not yet enabled, alternative information security measures, such as secure login protocols, continuous monitoring, and real-time threat detection, should be implemented, and any deficiencies assessed against APRA's material control weakness notification requirements.

Strategy for protection: Our member protection strategy combines advanced technology, proactive monitoring, and expert oversight to prevent fraud, scams, and other financial crimes.

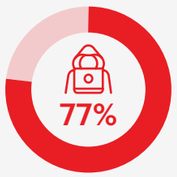
In addition, we have intensified monitoring across all systems and infrastructure, expanded SMS alerts for account changes, and implemented AI checks to detect unusual behaviour on member accounts. Continuous adaptation and enhancement of these measures are vital.

Our research findings showed that:

- Members are ready for secure, layered protection – but want it to be easy and reliable.
- Funds should also proactively communicate with members about the importance of using strong, unique passwords and avoiding credential reuse across systems.

Why digital ID is non-negotiable

While the Australian superannuation industry has made significant strides in securing the financial future of millions of Australians, the recent cyber incident and market disruption have highlighted the need for a united front against cybercrime.



Survey participants reported they had moderate to high concern after cyberattacks

61%

indicating they would be more loyal if security improved

55%

would consider switching due to experience or security concerns

This necessitates a strategic shift from reactive measures to proactive, stronger layered defences, with identity verification emerging as a key part of this change.

As members transition from accumulating to drawing an income from their super, funds face growing challenges in adapting to an increasingly digital world, particularly identity verification. While 69% of those surveyed use digital ID tools and MFA, their security behaviours are largely driven by platform design rather than personal initiative. For example, 60% of respondents said they would prefer to verify every time they log in, but many also want biometric ease and control over how and when they authenticate. 41% avoid complex setups, preferring simplicity – demonstrating the need for intuitive, flexible solutions.

In contrast, traditional paper-based systems that were once sufficient are no longer fit for purpose. Members today demand a more modern approach, including streamlined onboarding processes, secure data management, personalised services and communication, and proactive fund-to-member interactions and advice.

We believe the integration of robust digital identity solutions offers a dual advantage: significantly strengthening member protection against fraud and identity theft while simultaneously removing friction from critical member verification touchpoints throughout the superannuation journey.

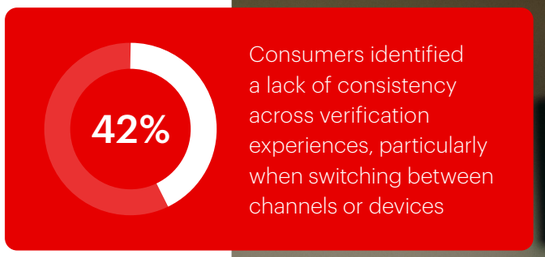
Verification touchpoints

From the moment they join a super fund to navigating various life stages and eventually accessing their benefits, there are numerous instances where identity verification is critical, but also frustrating for the member.

Top digital ID pain points for financial institutions include authentication failures and lack of fallback options, with 46% citing confusion over verification steps. For 42% of consumers, a lack of consistency across verification experiences, particularly when switching between channels or devices, was a frustration.

These frustrations may be compounded by outdated or manual processes, with some financial institutions having numerous touchpoints with a client during the onboarding process. Recognising this, most banking institutions acknowledge that successful Identity Verification (IDV) implementation is centred around enhancing customer experiences by streamlining the onboarding process[1].

The timeline on the following page outlines potential verification touchpoints across the life of a super fund member. It highlights interactions that typically require identity confirmation, ensuring strong security measures are in place at every stage, and ultimately demonstrating why digital ID is non-negotiable for enhancing security and efficiency in each of these moments.



Consumers identified a lack of consistency across verification experiences, particularly when switching between channels or devices

1. Fenergo. (July 2024). Digital Transformation is Changing How We Open Accounts

A member's life with a super fund

The growing threat of cybercrime along with increased regulatory scrutiny and members wanting easier digital interactions, presents super funds with some challenges to improve their digital capabilities.

Confidence in fund security remains modest – averaging just 3 out of 5 – highlighting the importance of visible security actions and user-friendly verification processes in maintaining member trust.

This extends beyond better cybersecurity; it also requires thinking about how member identity is verified throughout their time with the fund. In line with recent APRA guidance, authentication practices must now reflect both the criticality of member data and the evolving risk landscape.

Confidence in fund security rated moderate 3 out 5

To truly protect Australians' financial future and fix the problems with manual identity checks, super funds need better solutions. While 91% expect verification for high-risk transactions like withdrawals, 70% want it at onboarding, 67% expect it for standard logins and 63% when updating personal info details – revealing an opportunity for layered authentication that balances security with convenience.

This includes using advanced tools like verified credentials and biometric eVerification for KYC checks. These tools are key to making identity checks stronger, improving how members engage, and making payment processes smoother. A good first step to removing friction and making verification easier at every point is to widely adopt digital identity verification.

MUFG Retirement Solutions is committed to multiple streams of technology innovation in the identity space to transform these critical processes. We're looking at how verified credentials can change things, and we're actively making our current identity technologies better by moving towards biometric eKYC.

Touchpoints along the super journey

ONBOARDING	MONEY IN	ENGAGEMENT	MONEY OUT	ACCOUNT CLOSURE
• Account opening • Digital profile creation	• Employer contributions • Voluntary contributions • Consolidation & rollovers	• Online access • Investment selection • Insurance • Beneficiary updates • Financial planning & advice • Statements & communications • Member details updates • Pension payments	• Lump sum withdrawals • Insurance benefits • Hardship payments • Compassionate grounds • Early release scheme payments • Death benefits • Request to close account	• Final payment/rollover of remaining balance • Remove digital access

Our biometric eKYC pilot

For many funds, reliance on traditional identity verification methods, often involving manual, paper-based 100-point checks with multiple forms of physical ID, presents significant hurdles.

These methods are time-consuming, error-prone, and costly, causing frustration among members and substantial administrative burdens for funds. Furthermore, there are challenges with user experience, pass rates, and the security capabilities of some current identification solutions within the industry.

An innovative solution

Recognising these pain points, together with our clients we are trialling an innovative solution that tackles these challenges head-on. Our eKYC pilot program promises to not only improve efficiency and security but also significantly enhance the member experience.

This pilot program is testing an enhanced KYC process that leverages biometrics and facial recognition to check the authenticity of identification documents and match them against the member presenting identification via a smartphone user interface. The program streamlines member onboarding by verifying ID documents, matching personal details, and confirming member presence through a selfie comparison enhanced with liveness detection.

Data capture is automated via OCR (Optical Character Recognition), and additional verification checks are conducted based on risk. The program is compliant with AntiMoney Laundering (AML) regulations and is designed for future integration with services such as the Trust Exchange (TEx) initiative, Fraudulent Verification Services (FVS), and digital driver's licenses.

The tangible benefits of these modern identity verification approaches are already being realised across Australian industries with 82%[1] of businesses surveyed having already witnessed a reduction in fraud through identity verification technologies.

This impact is also financial, with AI-driven identity verification solutions credited with enabling Australian businesses surveyed to save an average of AUD $12 million[1] by preventing identity fraud. Specifically concerning biometrics, 84% of businesses affirm its efficiency in reducing fraud risks, with 36% considering it much more effective than current measures. These findings highlight the clear advantages for the superannuation industry.

Our pilot represents a critical step towards a more secure, efficient, and compliant verification solution, benefiting our clients, their members, and the broader super industry.

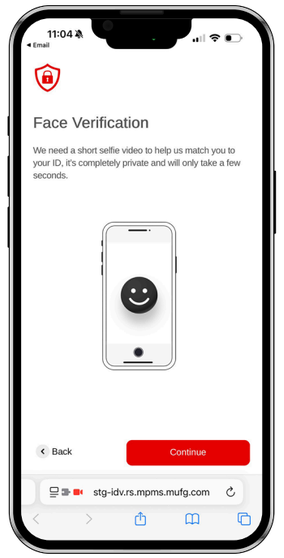
Benefits for super funds:

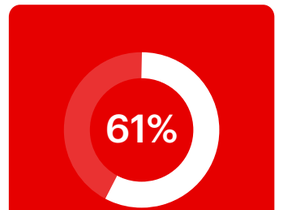
- Reduced operational costs
- Enhanced security and fraud prevention
- Improved member experience
- Strengthened regulatory compliance
- A competitive advantage
- Data breach mitigation

Benefits for the industry:

- Increased trust and confidence
- Potential for KYC standardisation
- Reduced fraud and financial crime
- Encourages innovation and technological advancement
- Improved efficiency and productivity across the industry

Example only

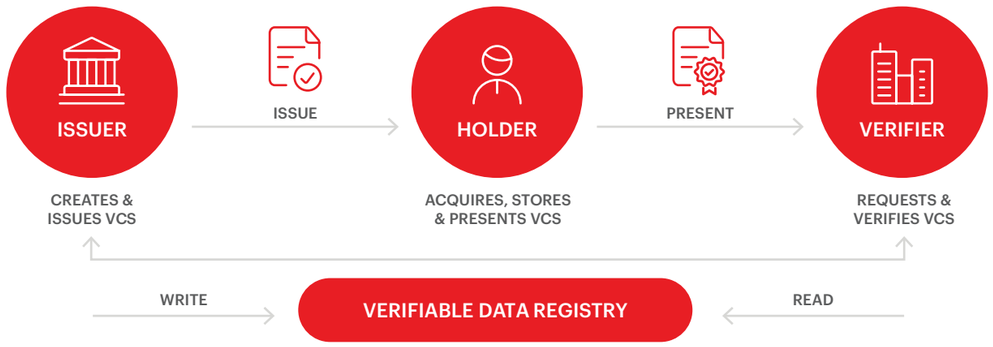




1. Docusign / Entrust. (Report cited by CFOtech Australia, April 2025)

Understanding verifiable credentials

The future of digital identity verification is likely to be built around verifiable credentials – digital equivalents of physical documents like passports or driver's licenses.



These credentials operate through a sophisticated yet straightforward process:

Issuance: An Issuer (e.g. a government agency) creates and issues a verifiable credential (VC) for the Holder (an individual), including details like name, date of birth, and a photo. The issuer signs the credential using a public cryptographic key.

Storage: The Holder securely stores the VC in a digital wallet on their smartphone, often secured by facial recognition or other biometrics.

Presentation: When needed, the Holder generates a "verifiable presentation" by selectively choosing specific information from their VC to share. The digital wallet sends this information to the Verifier.

Verification: The Verifier (e.g. a super fund) can instantly check the authenticity of the verifiable presentation using the cryptographic key, ensuring the received information matches what the issuer has securely stored on a Verifiable Data Registry.

This system builds upon existing government platforms like myGov and MyGovID, which many Australians already use for government services. However, the new approach takes this foundation to the next level, enabling more secure, privacy-preserving, and efficient information sharing for a wider range of uses.

Importantly, our survey showed that Australians are already familiar with digital identity sharing with 62% reporting regular use of digital ID tools with government agencies and banks, and another 34% use them occasionally. While cross-organisational sharing still triggers caution, clear controls and data transparency are seen as essential to increasing confidence.

Benefits of verifiable credentials

Implementing verifiable credentials delivers several key benefits for the superannuation industry:

Streamlined onboarding
Faster, more efficient onboarding processes with reduced administrative costs

Enhanced security
Stronger fraud prevention using secure, verified credentials

Better experience
Greater trust with control over personal data and access to bespoke financial services

Regulatory compliance
Meeting evolving data security and privacy regulations

Security Benefits: Protected by best-in-class encryption, individuals can share their information selectively, reducing the need for businesses and government agencies to store large volumes of personal data. This dramatically mitigates risks associated with data breaches, creating a safer digital environment for consumers and businesses alike.

Efficiency Benefits: Currently, financial services institutions must independently verify each member by checking various documents, often storing more information than they need. These manual processes can sometimes take five or more business days. Verifiable credentials streamline this process, automating it entirely, leading to significant time and cost savings.

Importantly for the private sector, verifiable credentials can improve the customer experience and directly address known cybersecurity and fraud risks such as impersonation and phishing. This aligns with broader sentiment: a study cited by Exadel in January 2024 found that 89% of financial services organisations believe passwordless authentication is a necessity, and 90% agree it offers cost benefits.

For clients of MUFG Retirement Solutions, we can leverage verifiable credentials to:

- Enable password-free logins
- Secure access to accounts
- Rapid processing of requests (e.g. benefit withdrawals)
- Power member loyalty and rewards programs, all while maintaining high levels of security

Leading the digital identity charge: International examples

Several countries are leading digital identity implementation through verifiable credentials, setting benchmarks for Australia's superannuation industry to follow.

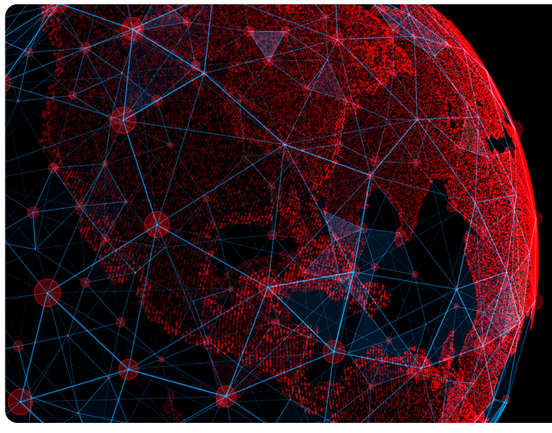
United Kingdom: The UK is advancing a government backed Digital Identity and Attributes Trust Framework linked to the European Wallet Consortium (EWC) to ensure EU interoperability, with the Digital Information and Smart Data Bill (2024) supporting these efforts. The National Health Service (NHS) uses VCs to manage qualifications and employee credentials, while GOV.UK One Login simplifies government service access.

Hong Kong: The iAM Smart platform provides residents with a single digital identity for accessing government services and conducting online transactions. It uses a mobile app for authentication and is specifically designed to integrate with an extensive range of public and private sector services.

Sweden: Citizens use Bank ID for everything from online banking and accessing retirement savings to interacting with government agencies and signing legal documents. The high level of trust and convenience associated with BankID has resulted in a thriving digital identity ecosystem.

Estonia: Stands as a global example of a comprehensive and integrated approach. Estonia's government-issued digital ID system uses verifiable credentials to connect banking, healthcare, and government services, creating a seamless digital experience. Singapore is currently transitioning to a similar VC-based model.

United States: US agencies including Citizenship and Immigration Services and Homeland Security are piloting VCs for immigration documents, while Apple is rolling out Digital Driver's Licenses built on VC technology. This signals growing federal and private sector adoption of verifiable credentials.



These international precedents, along with ongoing Australian initiatives such as the Digital ID Act, the 2024 Scams Prevention Framework, and the Trust Exchange (TEx) pilot with Services Australia, provide a clear roadmap and compelling evidence for the benefits that verifiable credential-based digital identity solutions can bring to the Australian superannuation landscape.

Future of identity verification: The Trust Exchange (TEX) initiative

The future of identity verification in Australian superannuation could lie in the recently proposed Trust Exchange (TEx) initiative, introduced by the Australian Government in August 2024.

What is TEx and why does it matter?

TEx builds on existing platforms like myGov and MyGovID, which are widely used for government interactions. However, it aims to go further by enabling secure, efficient sharing of personal information with a single click. Crucially, individuals maintain control over their data, sharing only what is necessary, when it is needed.

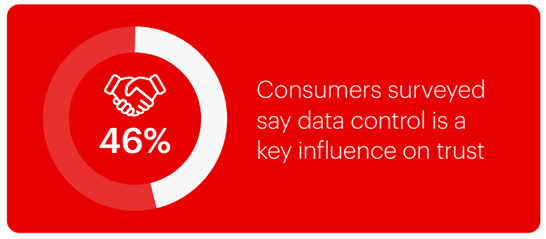
Initially piloted with the Department of Veterans' Affairs, organ donors, and other select groups, TEx plans to expand after a successful trial phase.

TEx in practice

At the core of TEx are verifiable credentials – cryptographically sealed, one-of-a-kind digital representations of personal information. Just as a passport serves as a trusted physical document, verifiable credentials offer a digital equivalent that can be authenticated by trusted authorities, ensuring both security and efficiency.

Leveraging myGovID, TEx facilitates secure sharing of verified credentials and personal data through digital wallets. This innovation could revolutionise the verification process for Australian retirees, empowering super funds to automate processes and provide faster, more reliable services across the entire member journey.

Members are particularly receptive when they know how their biometric data is stored, who can access it, and whether it stays in Australia. 46% of consumers we surveyed say data control is a key influence on trust, and official app-based communications are seen as far more trustworthy than generic emails.



By eliminating traditional, often manual, verification steps, TEx enhances privacy, minimises data storage (thereby reducing breach risks), and ensures compliance with evolving regulations.

It also addresses APRA's call for stronger, fit-for-purpose authentication measures – particularly in scenarios where traditional MFA may not yet be implemented or does not fully mitigate identity-related risks.

The industry's role in shaping TEx

The proof of concept for TEx was completed at the end of 2024, and with pilot programs now launched, we strongly encourage the industry to actively participate in its development once further documentation is released, ensuring its design meets the specific needs of the superannuation sector.

This call to action is especially important in the context of APRA's requirements, which reinforce the obligation to uplift authentication controls for high-risk activities and privileged access. Digital identity solutions like TEx directly support this regulatory expectation by offering a more secure, user-centric alternative to traditional credentials.

Super funds can realise the benefits of TEx digital identity with MUFG Retirement Solutions

At MUFG Retirement Solutions, we recognise the transformative potential of TEx and are committed to playing a proactive role in its implementation. By embracing verifiable credentials and other digital identity solutions, the superannuation industry stands to gain significant benefits, including:

Personalised services: Super funds can offer highly tailored solutions based on real-time, accurate, and consent-driven data, leading to more relevant and timely member interactions and advice.

Seamless integration: Digital identities simplify interactions across financial services, enabling flexible, member-centric solutions that break down traditional silos and create a more unified financial ecosystem.

Stronger authentication, fewer barriers: By replacing passwords, traditional MFA and repeat KYC processes with biometrics and secure digital wallets, the experience becomes simpler and safer for members.

Extensible across use cases: Beyond onboarding and identity verification, digital credentials can also support proof of entitlements such as fund membership, insurance eligibility, or loyalty programs.

Member control by design: Unlike traditional credentials, verifiable credentials allow members to share only the data required, when it's required, minimising over-disclosure and enhancing privacy. Importantly, copies cannot be reused or exploited.

AI-Powered efficiency: Advanced technologies like AI and machine learning can be integrated with digital identity systems to further automate verification processes, enhancing security and efficiency, and identifying unusual behaviours.

Tamper-Proof credentials: Verifiable credentials are sealed with cryptography, making them tamper-proof and verifiable without contacting the issuer, reducing friction while maintaining assurance of authenticity and currency.

Key considerations

Super funds should assess several critical operational and strategic priorities to support successful adoption.

- Integrating APIs with government platforms and other digital identity providers.
- Managing cryptographic keys and implementing robust security protocols to protect the integrity of the system.
- Ensuring that all identity verification protocols align with regulatory requirements.
- Training staff on new digital verification processes and member support for these new methods.

Preparing for the shift

Educating members will be essential to ensure they understand how digital identity works, recognise the benefits, and trust that their privacy and data remain protected under the new system.

Short videos, simple language guides, and opt-in choices are favoured over complex legal documents. Members want to know, in plain English, how it works and why it matters – 47% cite a preference for biometric-friendly options, and 52% say 'secure and reassuring' is their top expectation.

For super funds managing administration in-house, the transition to a digital identity framework like TEx may present operational challenges. These funds will need to adapt internal systems and processes, or partner with trusted administrative providers, to integrate these capabilities securely and efficiently.

Our commitment

Having completed its proof of concept at the end of 2024, and with pilot programs now launched, MUFG Retirement Solutions strongly encourages active industry participation and collaboration to ensure the retirement sector is well-positioned to leverage this innovation effectively.

Over the past six months, we have conducted capability and feasibility assessments for deploying digital identity technology. In partnership with Verified Orchestration, a local leader in verifiable credentials, we are identifying opportunities to innovate and engage proactively with federal and state governments on the development and implementation of these important initiatives.

These efforts are not only driven by a desire to improve member experience but also by a recognition of the regulatory imperative set out by APRA. Our approach ensures that emerging digital identity solutions are deployed in ways that comply with regulations and help super funds close critical gaps in authentication controls.

We remain committed to supporting the implementation of TEx, advocating for stronger security measures that prioritise consumer privacy, and advancing the superannuation industry for better outcomes for Australian retirees.

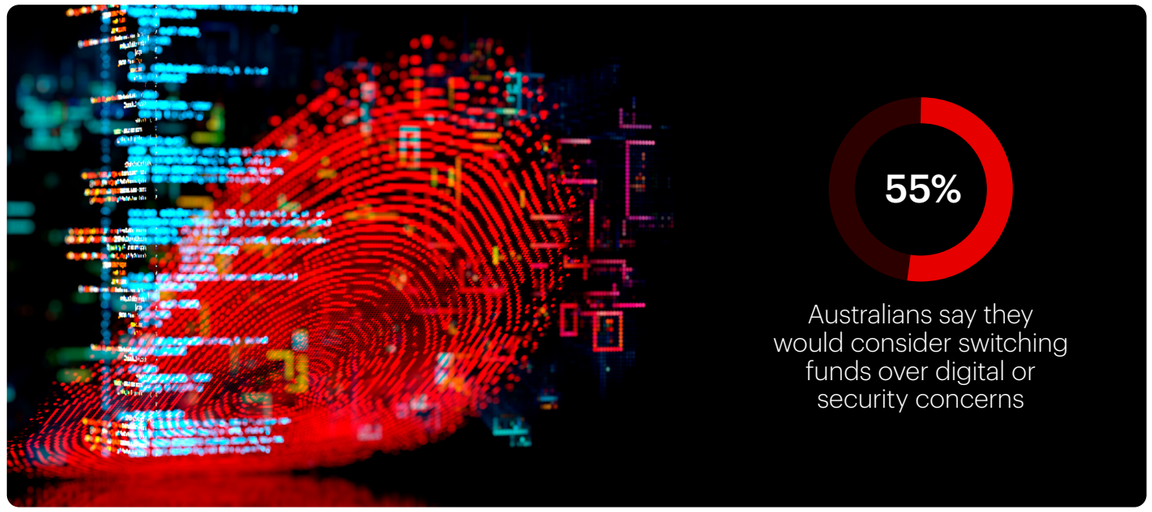
Conclusion

The recent cyber incident and market disruption served as a stark reminder of the escalating cyber threats facing the Australian superannuation industry. Our experience highlighted the critical importance of proactive cybersecurity measures, operational resilience, and the need for a united industry front in times of crisis. The efficacy of our ALERT system in protecting member data and funds provides a strong foundation as we explore new innovations to enhance operational impact.

Digital identity solutions, particularly biometric eKYC and the Trust Exchange (TEx) initiative based on verifiable credentials, represent an exciting leap forward. These technologies offer a dual advantage: they significantly boost protection for members by strengthening identity verification and combating fraud, while simultaneously removing friction from every touchpoint in the member journey – from onboarding to secure transactions and personalised interactions.

By supporting digital transformation in identity management, the superannuation industry can reduce operational inefficiencies, enhance member experience, encourage greater trust, and position itself for long term success in an evolving financial landscape. It is up to us, as an industry, to proactively lean into these innovations, ensuring the best possible results for members while contributing to a stronger, more resilient system that can support future generations.

As APRA's recent guidance makes clear, the time for action is now and uplifting authentication and identity controls is a fundamental obligation to protect the trust placed in us by millions of Australians.



References

- ACCC Scamwatch (2023). Scamwatch Report 2023.
- Australian Bureau of Statistics (ABS). (Published April 2025). Personal Fraud, 2023-24 financial year.
- Australian Cyber Security Centre (ACSC). (FY2022-23). Annual Cyber Threat Report.
- Australian Institute of Criminology. (July 2023). Identity crime and misuse in Australia 2023.
- Brankas. (May 2024). The Digital Transformation of Customer Onboarding in Banking.
- CFOtech Australia. (April 2025). Fraud against Australian businesses on the rise.
- Cybersecurity Ventures. (2022). Cybercrime Magazine Q3 2022.
- Digital Shadows. (Ongoing research). Dark Web Intelligence.
- Docusign / Entrust. (Report cited by CFOtech Australia, April 2025).
- Exadel. (January 2024). Digital Identity in Financial Services: Avoiding Fraud in 2024.
- MUFG Pension & Market Services (July 2025). Digital ID Research Report 2025
- Fenergo. (July 2024). Digital Transformation is Changing How We Open Accounts.
- IBM. (2023). Cost of a Data Breach Report 2023.
- Office of the Australian Information Commissioner (OAIC). (February 2025). Part 1: Data breaches and the Australian Privacy Act.
- The Australian Government. (August 2024). Trust Exchange (TEx) initiative announcement.

ABOUT MUFG RETIREMENT SOLUTIONS

MUFG Retirement Solutions is the leading provider of administration and technology services to the Australian superannuation industry. With a deep understanding of the regulatory landscape and a commitment to innovation, we partner with our clients to deliver secure, efficient, and member-centric solutions. Our expertise in cybersecurity, operational resilience, and cutting-edge digital identity technologies positions us as a trusted partner in safeguarding member assets and creating brighter retirement futures for all Australians.

MUFG Retirement Solutions
A division of MUFG Pension & Market Services

MUFG

201_0825