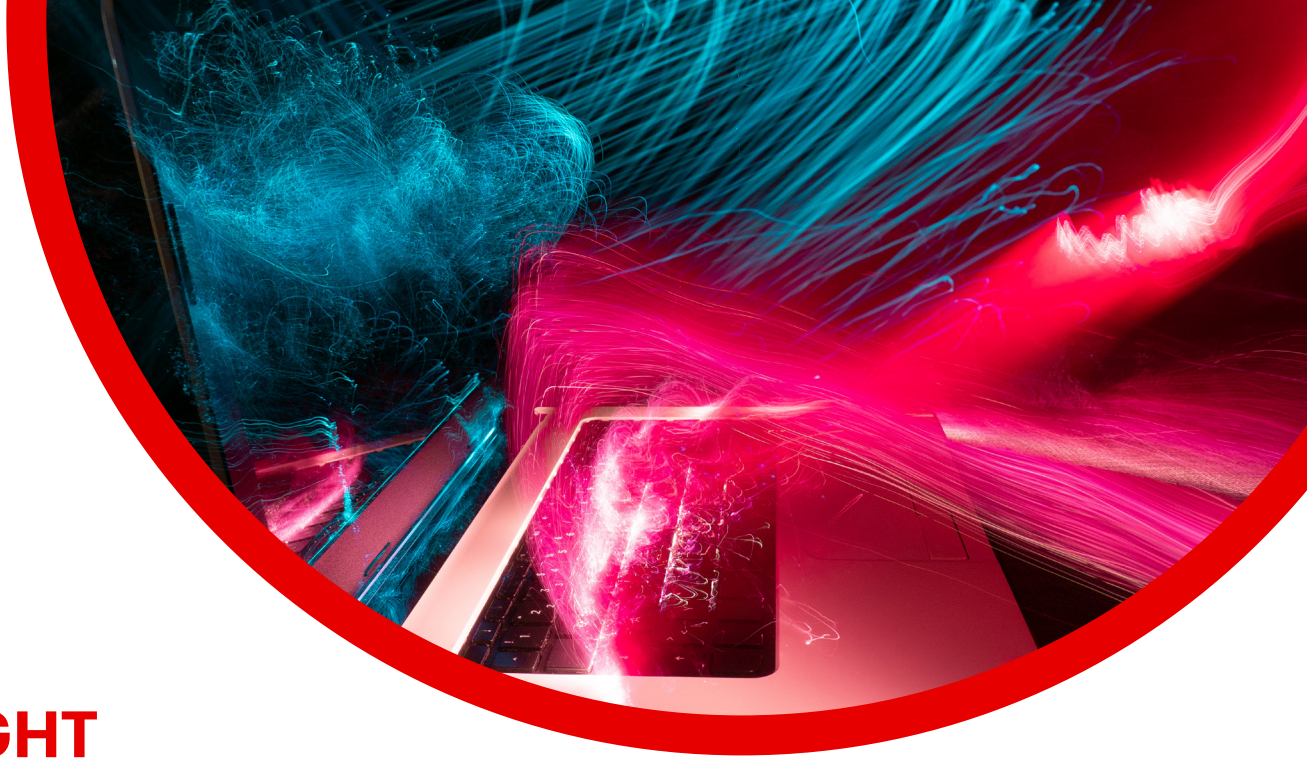


INSIGHT

Learnings from cyber & market disruption

MUFG Retirement Solutions identified an increase in threat activity over the weekend of 29 March 2025. Although indicators of threat activity were detected in parts of our environment, our security controls were effective and member data and funds remained secure. As a precaution, we implemented heightened monitoring to respond quickly to any potential threats.

Overview

Along with several funds, MUFG Retirement Solutions observed a significant increase in credential stuffing activity. This occurs when threat actors use compromised usernames and passwords from the dark web to attempt access to member accounts. On 4 April 2025, the issue attracted media coverage on cyber risks within the superannuation industry.

This cybersecurity threat coincided with global stock market turmoil following US trade policy changes to tariffs announced on 3 April 2025. US stock indexes saw their biggest daily percentage drops since the start of the COVID-19 pandemic in 2020, while the Australian market fell nearly 3% by 4 April 2025.

Intermittent performance issues affected multiple systems, including our member and contact centre portals. These issues were caused by a significant increase in member enquiries and transactions following the media attention, rather than malicious activity. Similar issues were experienced by funds and other providers, with some experiencing up to 700% more technical integration calls for digital services.

Our quick response, proactive risk mitigation, and experience managing similar events enabled us to collate insights for the broader superannuation industry to help foster a united front in times of crisis.

Cybersecurity monitoring insights

Our cybersecurity monitoring delivers real-time protection at scale - analysing hundreds of millions of data points daily to safeguard member data and assets, investigate suspicious activity, and prevent significant losses.

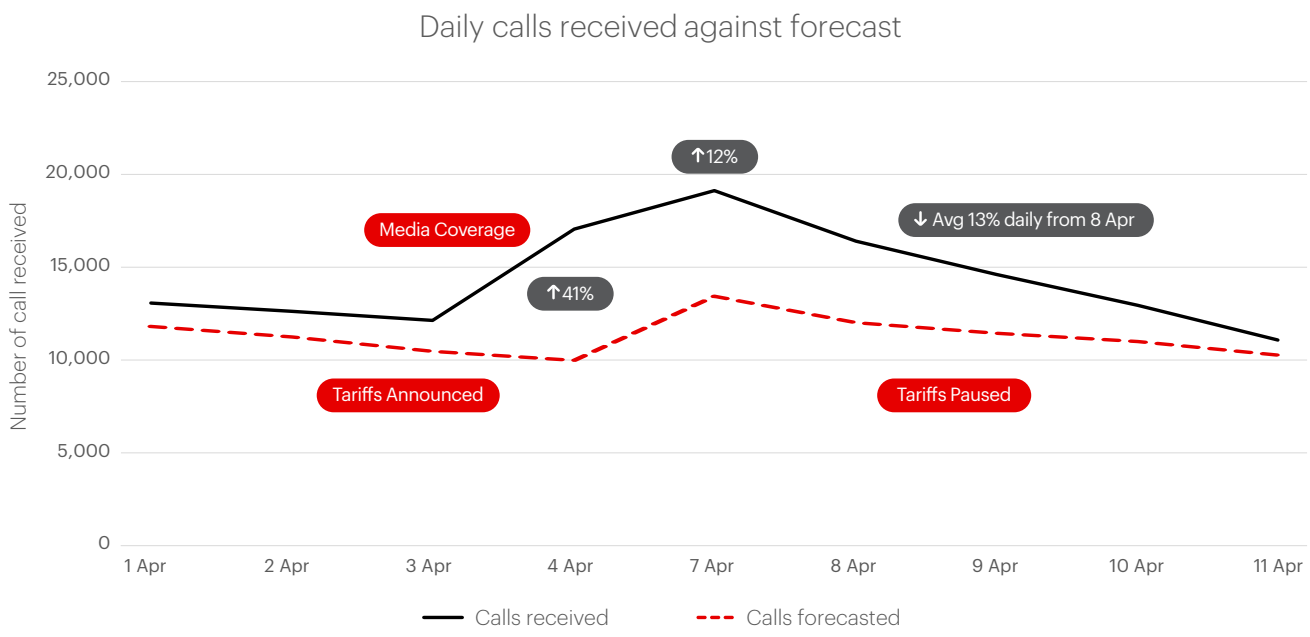
10m
Member Accounts
Actively Monitored

450m
Data Points Per Day
Data Analytics

$18m
Protected
Fraud Prevented

5k-10k
Accounts Investigated
Compromised

Member interaction insights



Call volumes increased by 41% on 4 April following media coverage and tariff announcements and rose by a further 12% on 7 April. Clear communication on protection measures and the 9 April pause on reciprocal tariffs drove a 13% average day-on-day reduction in call volumes.

25%
Calls were from members seeking information about the cyber threat, including concerns around security, fraud, and account safety

28%
Calls related to investment performance concerns driven by market volatility

Operational resilience & proactive management

The flow on impacts required immediate attention from our Crisis Management Team (CMT) along with frontline Services and Operations areas. It was also critical to keep regulators, funds and members informed through consistent and transparent communication as industry activity intensified.

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 320% compared to the previous week.

Extended hours, scaling to meet demand

- In consultation with funds, contact centres operated on the weekends of 5 and 12 April 2025.
- Workforce plans were executed to deploy resources and maintain critical services outside standard operating hours.
- Actively redirected appropriately skilled resources to high volume administration activities, leveraging our scale.

Partnering with funds for member assurance

- Collaborated with funds to ensure website and portal messaging addressed member concerns.
- Sent direct email communications to members to ease concerns about market volatility.
- Deployed fund-approved telephony-based messaging (IVR).

Insights for a united superannuation industry

Learnings from recent events should be used to establish a consistent approach to cybersecurity and support a united front in future crises.

Information security leaders network

- The superannuation industry needs to establish a Chief Information Security Officer (CISO) community that meets regularly to share experiences, exchange information and minimise risks across the broader industry. Security must be managed as a united front, taking cues from the banking sector.

One voice for the industry

- Media coverage surrounding the recent cybersecurity attack on Australia's superannuation industry significantly influenced public perception, often amplifying concerns beyond the actual scope of the incident.
- Such narratives, while based on real incidents, overshadowed the broader context that most accounts remained secure and that immediate actions were taken to mitigate risks.
- This highlights the importance of having one clear and consistent voice for the industry during such incidents to maintain public trust and prevent unnecessary panic.

Member portal access & MFA

- We strongly recommend deploying Multi Factor Authentication (MFA) to maximise security and proactively communicate with members about the importance of using strong, unique passwords and avoiding reuse of credentials across systems.
- Where MFA is not yet enabled, we have introduced a range of alternative information security measures, including secure login protocols, continuous monitoring, and real-time threat detection. Implementation would require discussion and agreement with each fund.

Strategy for protection and additional measures

- 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 members accounts.