Privacy breach 2022

30 May 2022

Spirit Super has contacted members affected by a data incident that has unfortunately resulted in some personal details being compromised. This article outlines what's happened and what Spirit Super is doing to support affected members.

Please note: If you haven't received an email, SMS or letter from Spirit Super about this incident then you haven't been identified as affected by this breach.

What happened?

On 19 May 2022, Spirit Super experienced a data incident where a staff member's email account was compromised.

We detected the information security breach and contained the account quickly. We've continued to investigate the extent of the breach, and we believe there was unauthorised access to a mailbox containing personal data.

The personal data that may have been compromised is similar to some information provided in an *annual statement*, including names, addresses, ages (as at 2019 and 2020), email addresses, telephone numbers, member account numbers and member balances (as at 2019 and 2020).

It's important to note that this data **DOESN'T** include dates of birth, government identification numbers (such as tax file numbers or driver's license details), or tax file numbers or any bank account details.

The breach was the result of an email phishing activity, rather than a system error, regardless we're taking all reasonable steps to prevent this from happening again.

Please be assured investigations to date indicate that accounts haven't been compromised. We've increased the levels of security to ensure our members' accounts remain safe. Our investigation will continue.

What are we doing?

Spirit Super takes cybersecurity and the protection and privacy of our members' data extremely seriously. We moved immediately to secure accounts and member data.

We're undertaking a thorough investigation to assess the impact. This includes reviewing account activity and placing enhanced controls on accounts.

We're also notifying all relevant authorities, including the Privacy Commissioner, and will work with them in a transparent manner.

We'll take immediate precautions to further strengthen our IT security and reduce future risks of cyber incidents

I'm worried, who can I speak to about this?

We understand that members may feel worried about this breach, and how it may affect them personally. Please be assured that our members are our highest priority, and we want you to be aware that we have, and will continue to, work to assess and contain the situation as our top priority. We deeply regret this incident, and sincerely apologise to members who may have been affected by this data breach.

General inquiries can continue to be made to the Spirit Super Contact Centre on **1800 005 166**.

If there is any further information that comes to light, we'll let you know on our website at **spiritsuper.com.au/privacy-breach-2022**.

Frequently asked questions

How did this happen?

In short it was human error during a malicious email attack posing as official correspondence. This wasn't the result of a material security control weakness or technology failure. The malicious email resulted in a staff member's password being compromised.

Spirit Super employs multi-factor authentication (MFA) in addition to a username and password to access our systems. Unfortunately, this additional layer of protection was overcome by the attacker and the mailbox was accessed. Phishing attacks such as this are becoming increasingly sophisticated and common.

We have a skilled internal team focused on cyber security and protecting your information. This team detected the compromised account and acted quickly to contain and limit the impact of the breach. No further accounts or systems were impacted.

Was this a targeted attack?

No. We believe this wasn't a targeted attack. Quite the opposite, we believe that Spirit Super has been caught up in a broad phishing attack campaign.

Why was my data in the mailbox?

We're reviewing all our data handling practices and staff training. As a member focused organisation, for various reasons our staff are required to handle member data. Regrettably, some of this data from 2019-20 was contained within the compromised email mailbox.

While we know the malicious party had access to the mailbox, they may not be aware that they have this information. We can't speculate on their motive for the original attack.

Do we know if my information has been accessed?

We have no evidence to suggest your information and the broader set of member data has been intentionally accessed. All we know is that the email account was compromised, and within that mailbox this data was available. The attacker may not be aware of the data set. Because of this, we recommend limiting any activity that might draw attention to your details being included in the data set, such as posting on social media.

Is my money safe?

Yes. Your money is safe. We increased our security controls immediately following this breach. This includes increased identification steps on the accounts of impacted members. We have proactively implemented a block to payments from these accounts as a precaution. Please contact us if you have a need to withdraw money from your account and are eligible to do so. We aren't aware of any unauthorised activity to member accounts.

Note for pension members: The block to payments doesn't apply to established regular pension payments that are going to the usual bank account, these payments will continue as normal.

Has there been any suspicious account activity since the breach?

No. We have no evidence of suspicious activity since the breach. We've analysed account activity for impacted members specifically looking for unusual activity with nothing identified to date. We continue to monitor all impacted members' accounts in addition to our block on payments to minimise any risk of fraudulent access of funds. Fraud monitoring and controls are a regular aspect of our business and remain in place to protect all member accounts from unauthorised activity.

The compromised data isn't sufficient enough on its own for someone to access your Spirit Super account.

How do I know if I am affected by this privacy breach?

At this point, the majority of impacted members have received an email. SMS has been used to notify members where no email address was recorded. We're writing to a small number of individuals where email or SMS wasn't available. All impacted members will receive a letter notifying them as soon as possible.

How many members were impacted?

The impact to individual members is limited to the information shared below. We've reported the scope of the incident to the required authorities. The number of members impacted is approximately 50,000 records from 2019-20.

Why wasn't I notified sooner?

Spirit Super took appropriate response measures at the time the email account was compromised. Once we identified that a privacy breach had occurred and the scope of the incident had changed, we immediately began the process of implementing additional measures to protect our members and preparing communication to affected members. We alerted impacted individuals as soon as we could following discovery of the privacy breach. Our monitoring and investigation continues.

What should I do?

Remain vigilant to unsolicited emails, text messages or phone calls. If you do receive contact that you believe to be suspicious don't provide information to the caller. Contact Scamwatch to report the matter (**scamwatch.gov.au**).

There's no need to change passwords for your **Member Online** account as these weren't accessed. You can of course change this if you're concerned. Multi-factor authentication is required for sensitive account transactions to protect your information and keep you safe.

We would also suggest that you don't share that your personal information may have been compromised online or on social media to reduce your chances of becoming a target for further activity. We encourage members to be aware of any sensitive personal information they may have within their social media profiles that could be publicly available – such as date of birth.

Please remember that this advice applies more broadly than just in relation to your Spirit Super account. If you receive unsolicited contact we recommend verifying the contact prior to responding.

What specific information was contained in the breach?

The dataset included the following information, noting that not all members have all of these details in our systems. The information in the dataset was from June 2019 and June 2020 and not current information:

- member number
- title
- first name
- surname
- email address
- home phone
- mobile phone
- address
- age (but not date of birth)
- account balance.

What can be done with the information?

There were no government identifiers in the data and there's minimal risk of identify theft or fraud as a result of the limited data set involved in the privacy breach. Typically, 100 points of ID are required for someone to apply for a credit card or take out a loan. This information set doesn't provide that level of information. There was also no password or password clue information (such as mother's maiden name) or other information typically needed to confirm your identity with a financial institution. There were no dates of birth.

It's possible that the information could be used to contact you in an attempt to get you to disclose further information, such as your date of birth. This is why we recommend you remain vigilant.

The data is dated June 2019 and June 2020, limiting the currency of some of the information within.

Will you change my member number?

No passwords were accessed through this breach. We aren't recommending changing member numbers. Changing account numbers isn't necessary and may have unintended consequences, for example implications with any Centrelink entitlements for members in pensions phase.

What is being done to prevent this from happening again?

Spirit Super takes your privacy and the security of our information and systems extremely seriously. Online threats are constantly evolving, and no organisation can completely mitigate these risks. We continue to invest in internal capability, technology, improved internal processes, and staff training to reduce the likelihood and severity of future data breach events. In the immediate term, we'll be communicating with all staff and providing guidance on enhanced measures when handling sensitive information, and taking extra precautions around multi-factor authentication prompts.