



On 21 July 2020, the United Workers Union experienced a ransomware attack. A system was compromised which contained a list of members. The list included the data described in the following table. It is not known if the attacker downloaded the list.

Field	Description
Name	Member's first and last name
Financial Status	A Y/N field indicating union membership financiality
Payment Status	Detail about financial status e.g. Paying, Bad Account, Covid-19 Waiver etc.
Gender	Gender
Payment Type	Method of payment e.g credit card, direct debit, payroll deduction etc...
Payment Frequency	Frequency of payment e.g. weekly, monthly, yearly
ATSI	Aboriginal or Torres Strait Island status
State Electorate	Australian state electorate
Federal Electorate	Australian federal electorate
State	Address state
Join Method	How the member joined - online, phone, organiser conversation etc...
Site	The name of the member's place of work sometimes containing the suburb
Employer	The name of the member's employer
Employment Type	Full time, part time, casual etc
Occupation	Occupation where known - Teacher Assistant, Driver etc...
Member Leader	A Y/N field indicating an active role in the union
Age Cohort	Banded age e.g. 25 and under, 26 to 35, 36 to 45 etc...
Organiser	Assigned organiser
Transactions	A list of union payments since Feb 2020

The list did NOT include credit card information, bank details, usernames, passwords, email addresses, phone numbers, address information, dates of birth, or other identity information.

For more information, please email privacy@unitedworkers.org.au