Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

ReportCyber

version: 10.0.0

Your ReportCyber Receipt

Thank you for reporting. The reference number for this report is: **CIRS-20220807-110**. You can provide this number to financial institutions or other organisations as proof that a report has been submitted to police via ReportCyber at cyber.gov.au/report.

Your ReportCyber Receipt will also be emailed to you at the email address you provided in your report. For privacy reasons, a summary of your report cannot be emailed, but you can download it:

Downloading your report allows you to have a copy of your report for your records. Note: once you close this page, you will not be able to get a copy of your report.

Support services are available

Cybercrime can be distressing and may have a severe impact on mental health.

If you or someone you know has been affected by cybercrime and is struggling, professional support is available.

For matters requiring urgent Police attention, contact (000).

For support contact Lifeline (13 11 14) Beyond Blue (1300 22 4636) or Kids Helpline (1800 55 1800) - available 24 hours a day, 7 days a week

This report has been referred to the NSW Police Force for assessment. If you have any queries about your report you can contact them at reportcyber-enquiry@police.nsw.gov.au

If you would like to check the status of your report in the future, you can visit the Report Status Check web page and follow the instruction.

The Australian Cyber Security Centre (ACSC) will be unable to advise you on the progress of your report as it has been referred to NSW Police.

Please note that not all matters will be investigated by Police, but all reports are important to us as they may provide information on the latest crime trends. Due to the complex nature and large volume of reports we receive, there may be a delay before you are contacted if your report is assessed to be suitable for police investigation. If you believe your matter requires urgent attention, please attend your local police with a copy of this email.

Domestic Violence or Personal Violence related matters should NOT be reported on this system regardless of any cyber related factors. Please contact your local Police for assistance if you are in a domestic violence situation or call 000 if there is an immediate threat to life or risk of harm.

Based on the information provided, someone may have fraudulently used your identity.

What to do now:

- Contact your bank immediately if you have sent money or if you think you have provided confidential banking information to someone online.
- Contact IDCare (idcare.org) to help recover your identity.
- Run a full scan on your device using your anti-virus software and follow the instructions to remove any identified files.
- Change your passwords.

What to do to prevent this issue from happening:

- Configure your email to require two-factor authentication (eg password plus a code sent via SMS)
- Never give anyone your username or password or let anyone access your online accounts. Use different passwords for each of your accounts.
- If your personal information was exposed in a data breach, report to the organisation that shared your information and change your account passwords.

To better understand the issue, visit the following sites:

- Visit cyber.gov.au for more information
- IDCare

Report details

What happened

Events that may have led to theft of your personal identity information

You received a phone call requesting access to your device

Events indicating use of your personal identity information

You received bills, invoices or receipts for goods or services you haven't purchased

Date you became aware of the issue	29/07/2022
Other financial losses caused by use of personal identity information	Bills in your name

Details of bills

Service provider	Vodafone
Total value of bills in Australian dollars	$2,000
What evidence do you have?	Copy of email communications, Text messages / Call recordings
Did you visit a police station or call the police about this issue?	No

Suspect details

Do you have details including account details or billing address?	Yes

Were fraudulent accounts opened in your name?	Yes
What fraudulent accounts were opened in your name?	Telecommunications

Telecommunications account details

Account provider	Vodafone
Account number	955759394

Description of events

Description

I received a call from Vodafone customer care on 03-Mar-2022 for free iPhone 13 Pro upgrade as my iPhone 12 plan was completing in March 2022. The order was placed and I received an email confirmation on the new order booking. I received a message in a week that the order was delivered whereas I did not receive any package. I checked with the Vodafone customer care (1555) for the order twice or thrice. I was told the order was misplaced and gave new order processing number for the second time. I was checking Vodafone customer care more often and I was asked to wait for the delivery as there were more orders being delivered. Finally, received a call from Vodafone asking for NBN upgrade where I was requesting for iPhone 13 on 14-June-2022 and came to know it was a fraudulent Transaction. I'm paying the monthly bill of AUD 120 and above which includes monthly plan of iPhone 13.

Contact details

Please choose an option	I am the victim

Your details

First name	Vaidyanathan
Last name	Radhakrishnan
Gender	Male
Date of birth	15/04/1980
Physical address	ATRIA ON COWPER UNIT 1705 36-46 COWPER ST, PARRAMATTA NSW 2150
Contact number	0405370561
Email address	vaidyanathan.radhakrishnan@gmail.com
Do you have any special needs or requirements?	No
Are you of Aboriginal and/or Torres Strait Islander descent?	No
Do you want police to investigate this matter?	No