Fujitsu General Australia

ABN: 55 001 229 554

Eastern Creek Drive, Eastern Creek NSW 2766
PO BOX 6504 Blacktown NSW 2148

t 02 8822 2500 w fujitsugeneral.com.au
f 02 8822 2501

30th January 2019

Dear Online Account Holder,

Information about a cyberattack on Fujitsu General Australia's online spare parts e-commerce store

You are receiving this letter/email because you have transacted with Fujitsu General's online Spare Parts eCommerce store.

On 16 January 2019 we became aware of information suggesting that our online store had been subject to a sophisticated cyberattack. A detailed forensic investigation is currently ongoing.

We are writing to provide you with the most current and best understanding of what has happened.

1 What happened?

The information we have received so far indicates (All times mentioned are in AEDT):

- A brute force attack appears to have taken place on 27 December 2018.
- The attack appears to have compromised the security controls on the online store and enabled the creation of an unauthorised administrative account.
- The system was protected by a server side scanner and malware scanner. There was no detection of any issue until 11:23 pm on 15 January 2019 when the malware scanner issued a warning to Leafcutter. An email formally advising Fujitsu General of the incident was issued by Leafcutter at 10:00 am on 16 January 2019.
- Malware known as MW:BLK:2 was identified by the Sucuri scanner on the site.
- Detection of the malware was observed by Fujitsu General staff at 8:00 am, with the solution provider providing notice by 8:45am on 16 January 2019. We shut down the site to customer access by 9:00 am on 16 January 2019.

2 What are we doing?

When we were informed of the incident, we immediately suspended operation of the ecommerce store.

ABN: 55 001 229 554
Eastern Creek Drive, Eastern Creek NSW 2766
PO BOX 6504 Blacktown NSW 2148
t 02 8822 2500 w fujitsugeneral.com.au
f 02 8822 2501

We obtained a forensic report from our solution provider, Leafcutter, and have since engaged a forensic expert to fully analyse the event and a penetration tester to test and help us to remediate the security of our new version of the online store.

We are using a code repository snapshot of the compromised site to re-establish an operating site using back-up files created in September 2018, before the compromise took place.

The new site will have additional security measures (server level and platform level). Once checked and tested we hope to relaunch the site as soon as possible.

We have notified the Office of the Australian Information Commissioner.

3 What information may have been accessed?

Information associated with your account may have been exposed and/or copied. The information potentially compromised is the information associated with your account including name, address, telephone number, e-mail address, ARCTICK licence number, ABN number and details of purchases you have made using the site. We currently have no direct evidence that your information has been accessed or copied but this appears to be a real possibility considering the level of access achieved by the attacker.

Payment and bank account information is held separately, however, if you made a credit card purchase between 27 December 2018 and 16 January 2019 your credit card details may have been intercepted.

What can you do?

If you made a credit card purchase between 27 December 2018 and 16 January 2019, we recommend that you immediately:

- check the transactions on your account and request that your credit card provider decline any transactions that appear fraudulent.
- request that your credit card provider cancel your credit card and issue a replacement.

Even though there is no evidence that your password has been compromised, we recommend that you consider updating your password/s particularly if you use the same password for other

ABN: 55 001 229 554
Eastern Creek Drive, Eastern Creek NSW 2766
PO BOX 6504 Blacktown NSW 2148
t 02 8822 2500 w fujitsugeneral.com.au
f 02 8822 2501

online services. We also recommend you maintain an ongoing check of your accounts for any unusual transactions or activity.

Make sure you have up to date virus checking software and run a full system scan on all machines that may have logged in to our online store on or after 27 December 2018.

Please be vigilant regarding potential phishing emails and scam telephone calls. In particular:

- check the sender address of all emails that contain links or attachments to ensure they come from the purported sender.
- do not open links or attachments on any email that appears to come from a unique or doubtful email address (perhaps because it is not the usual email address for the purported sender, or it has a misspelling or is unrelated).
- do not open links or attachments on any email that you were not expecting, or which looks inauthentic in any way.
- obtain identity verification and insist on calling back any caller you don't recognise.

We will advise you if our investigations indicate that any of this information is incorrect or we uncover additional information.

We are taking this matter very seriously and sincerely apologise for the inconvenience and concern this may cause.

Regards,

Philip Perham
Managing Director
Fujitsu General Australia

If you have any questions, please contact privacy@fujitsugeneral.com.au and we will endeavour to respond in a timely manner.

For general information about how you can protect your data privacy, visit **the Australian Competition and Consumer Commission's ScamWatch website**