Park'N Fly notifies 1 million customers of data breach

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

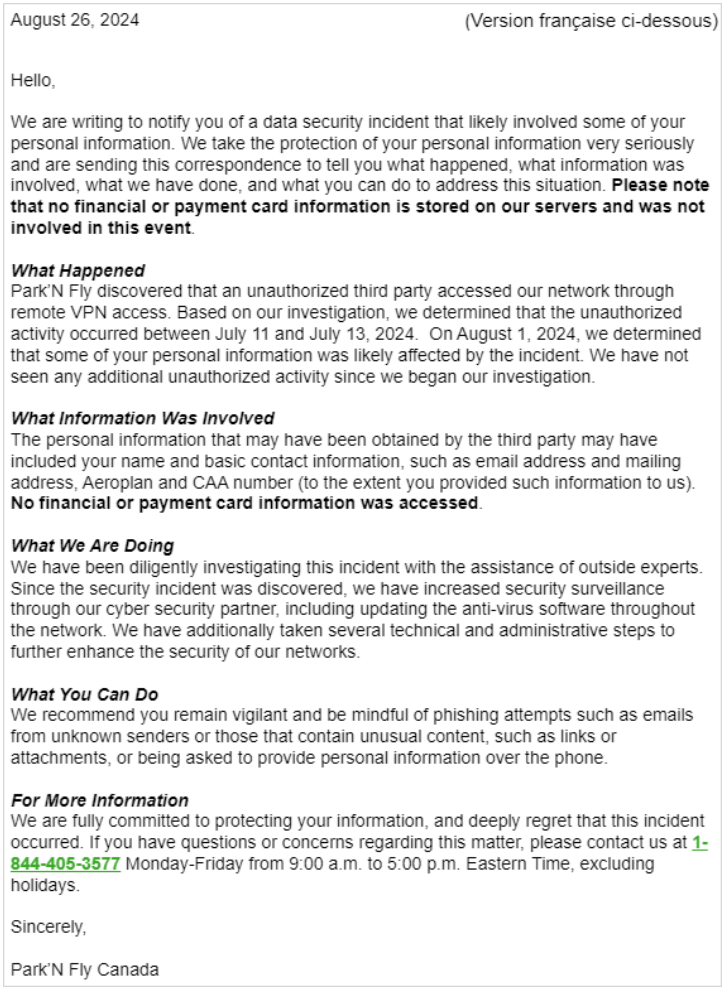
August 27, 2024 11:24 AM 1

Park'N Fly is warning that a data breach exposed the personal and account information of 1 million customers in Canada after hackers breached its network.

The threat actors breached the Park'N Fly networks through stolen VPN credentials in mid-July and stole data from the company. On August 1, the company determined that customer information was also accessed during the attack.

"Park'N Fly discovered that an unauthorized third party accessed our network through remote VPN access," reads the notice sent to customers and shared with BleepingComputer.

"Based on our investigation, we determined that the unauthorized activity occurred between July 11 and July 13, 2024. On August 1, 2024, we determined that some of your personal information was likely affected by the incident."



August 26, 2024 (Version française ci-dessous)

Hello,

We are writing to notify you of a data security incident that likely involved some of your personal information. We take the protection of your personal information very seriously and are sending this correspondence to tell you what happened, what information was involved, what we have done, and what you can do to address this situation. **Please note that no financial or payment card information is stored on our servers and was not involved in this event**.

What Happened
Park'N Fly discovered that an unauthorized third party accessed our network through remote VPN access. Based on our investigation, we determined that the unauthorized activity occurred between July 11 and July 13, 2024. On August 1, 2024, we determined that some of your personal information was likely affected by the incident. We have not seen any additional unauthorized activity since we began our investigation.

What Information Was Involved
The personal information that may have been obtained by the third party may have included your name and basic contact information, such as email address and mailing address, Aeroplan and CAA number (to the extent you provided such information to us). **No financial or payment card information was accessed**.

What We Are Doing
We have been diligently investigating this incident with the assistance of outside experts. Since the security incident was discovered, we have increased security surveillance through our cyber security partner, including updating the anti-virus software throughout the network. We have additionally taken several technical and administrative steps to further enhance the security of our networks.

What You Can Do
We recommend you remain vigilant and be mindful of phishing attempts such as emails from unknown senders or those that contain unusual content, such as links or attachments, or being asked to provide personal information over the phone.

For More Information
We are fully committed to protecting your information, and deeply regret that this incident occurred. If you have questions or concerns regarding this matter, please contact us at **1-844-405-3577** Monday-Friday from 9:00 a.m. to 5:00 p.m. Eastern Time, excluding holidays.

Sincerely,

Park'N Fly Canada

Park'N Fly notice to customers
Source: BleepingComputer

Park'N Fly is a large provider of off-airport parking services in Canada, offering travelers a convenient place to park their cars when flying out of major airports across the country.

The firm, which also offers shuttle, car washing, and oil change services, operates facilities located near airports in Toronto, Vancouver, Montreal, Edmonton, and Ottawa.

The information that has been exposed in this includes full names, email addresses, physical addresses, aeroplan number, and CAA numbers.

Park'N Fly says that no financial or payment card information has been exposed.

A spokesperson for the company told BleepingComputer that approximately "1 million customer files were accessed," noting that account passwords remain secure.

Impacted systems were fully restored within five days, stated the spokesperson, adding that they are implementing additional security measures to safeguard user information in the future.

"While we deeply regret any concern this incident may have caused, we want to reassure our valued customers and partners that we are taking all necessary steps to safeguard their information," stated Park'N Fly's CEO, Carlo Marrello.

"We remain committed to transparency and will continue to prioritize the integrity of our systems as we navigate this situation."

Customers who received letters took to Reddit (https://www.reddit.com/r/canada/comments/1f1w07c/parkn_fly_data_breach_included_personal/) to vent their frustration by yet another data breach impacting them, questioning the established practice of companies keeping customer data around for long after the service has been offered.

Some noted that the leak of Aeroplan numbers could easily lead to account hijacks, advising password resets for those participating in Air Canada's frequent-flyer program.

Park'N Fly warns impacted customers to remain vigilant and watch out for phishing attempts from unknown contacts, either via email or phone calls.

H/T Gerry Corcoran

Related Articles:

Dairy giant Agropur says data breach exposed customer info (https://www.bleepingcomputer.com/news/security/dairy-giant-agropur-says-data-breach-exposed-customer-info/)

BlackSuit ransomware stole data of 950,000 from software vendor (https://www.bleepingcomputer.com/news/security/blacksuit-ransomware-stole-data-of-950-000-from-software-vendor/)

Patelco notifies 726,000 customers of ransomware data breach (https://www.bleepingcomputer.com/news/security/patelco-notifies-726-000-customers-of-ransomware-data-breach/)

CannonDesign confirms Avos Locker ransomware data breach (https://www.bleepingcomputer.com/news/security/cannondesign-confirms-avos-locker-ransomware-data-breach/)

FlightAware configuration error leaked user data for years (https://www.bleepingcomputer.com/news/security/flightaware-configuration-error-leaked-user-data-for-years/)

AIRPORT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/AIRPORT/)

CANADA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CANADA/)

CUSTOMER DATA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CUSTOMER-DATA/)

DATA BREACH (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DATA-BREACH/)

PARK'N FLY (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PARKN-FLY/)

PARKING (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PARKING/)

(https://www.bleepingcomputer.com/author/bill-toulas/)

BILL TOULAS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/BILL-TOULAS/)

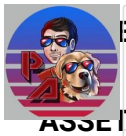
(MAILTO:BILL.TOULAS@BLEEPINGCOMPUTER.COM) **(HTTPS://TWITTER.COM/BILLTOULAS)**

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

PREVIOUS ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/MICROSOFT/WINDOWS-ENTIFY-UNKNOWN-ASSETS-WHILE-PEN-TESTING/)

NEXT ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/MICROSOFT/WINDOWS-DOWNDATE-TOOL-LETS-YOU-UNPATCH-WINDOWS-SYSTEMS/)

Comments



PXAbstraction (https://www.bleepingcomputer.com/forums/u/1180979/pxabstraction/) - 14 hours ago

Cheers Bill! Glad I could put this on your radar. Thanks for helping spread word. As someone who used Park N' Fly 4 months ago, I am just tickled pink by this.

Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

You need to login in order to post a comment

Login

Not a member yet? Register Now (https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register)

POPULAR STORIES

Microsoft: Exchange Online mistakenly tags emails as malware
(https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-online-mistakenly-tags-emails-as-malware/)

Seattle-Tacoma Airport IT systems down due to a cyberattack
(https://www.bleepingcomputer.com/news/security/seattle-tacoma-airport-it-systems-down-due-to-a-cyberattack/)

FOLLOW US:

(https://www.bleepingcomputer.com)

MAIN SECTIONS

News (https://www.bleepingcomputer.com/)

VPN Buyer Guides (https://www.bleepingcomputer.com/vpn/)

SysAdmin Software Guides (https://www.bleepingcomputer.com/sysadmin/)

Downloads (https://www.bleepingcomputer.com/download/)

Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)

Tutorials (https://www.bleepingcomputer.com/tutorials/)

Startup Database (https://www.bleepingcomputer.com/startups/)
Uninstall Database (https://www.bleepingcomputer.com/uninstall/)
Glossary (https://www.bleepingcomputer.com/glossary/)

COMMUNITY

Forums (https://www.bleepingcomputer.com/forums/)
Forum Rules (https://www.bleepingcomputer.com/forum-rules/)
Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)
Sitemap (https://www.bleepingcomputer.com/sitemap/)

COMPANY

About BleepingComputer (https://www.bleepingcomputer.com/about/)
Contact Us (https://www.bleepingcomputer.com/contact/)
Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)
Advertising (https://www.bleepingcomputer.com/advertise/)
Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)
Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)
Changelog (https://www.bleepingcomputer.com/changelog/)

Terms of Use (https://www.bleepingcomputer.com/terms-of-use/) - Privacy Policy (https://www.bleepingcomputer.com/privacy/) - Ethics Statement (https://www.bleepingcomputer.com/ethics-statement/) - Affiliate Disclosure (https://www.bleepingcomputer.com/affiliate-disclosure/)

Copyright @ 2003 - 2024 **Bleeping Computer® LLC (https://www.bleepingcomputer.com/)** - All Rights Reserved