From: The C-MAP Team <service@m.cmap.com>
Sent: Monday, October 2, 2023 5:53 AM
To: Rudy Guenoun
Subject: TEST - Formal Notification – NT/PC C-Map store/Navico Group IT Security Incident

Dear NT/PC C-Map store user,

Notification of IT security incident

Navico Group, (a division of Brunswick Corporation) has experienced an IT security incident ("**Incident**") impacting our online NT/PC C-Map store.

As a previous user of the online NT/PC C-Map store, some of your personal information was stored in this system, so please take the time to read this email carefully. We strongly encourage you to take the steps set out in this email, and want to assure we are working diligently to support you, address the incident and restore our service. Navico Group apologises for the concern and inconvenience this may cause you.

What has happened?

On or around 9 June 2023, Navico Group experienced an Incident. We promptly commenced an investigation into the Incident, and subsequently determined that an external threat actor had gained unauthorised access to certain IT systems including the online NT/PC C-Map store.
The following types of information about you may have been stored in the online NT/PC C-Map store, and it is possible that the unauthorised third party accessed this information:

- name;
- contact information (physical address, email address, phone number);
- billing address and payment token (partial/masked – non-usable credit card number); and
- password.

Steps taken by Navico Group to address the Incident

We have taken the following steps to address the Incident:

- as soon as the Incident was discovered, we restricted access to our systems and initiated an investigation into the cause of the suspicious activity;
- we engaged external advisors to assist in our investigation;
- as the extent of the Incident became known, we took all of our internet-facing services

offline;
- we applied additional security settings;
- we deleted passwords from the database; and
- we reported the Incident to Data Protection Authorities where required.

Steps you should take

Although at this stage we are not aware that any of your information has been misused, and we have no reason to believe that this will happen in the future, as a precaution, we recommend you take steps to actively monitor your email accounts for any unusual activity and to adopt a heightened awareness, including by:
- changing your password on any online services where you used the same password;
- wherever possible, ensuring that your online accounts are protected through use of multi-factor authentication;
- always exercising good password hygiene;
- being on the lookout for scammers who may try to access your personal information, for example, by way of suspicious emails, texts, phone calls or messages on social media. Never respond to such approaches;
- not clicking on any links that look suspicious, and never providing your passwords to anyone;
- never allowing anyone to access your computer (even if the person says that they are from a credible organisation); and
- subscribing to services made available to you by local authorities for the latest information about scams impacting our community.

For more information about the data security options that may be available to you, please see our Data Security Measures and Information webpage, available here.

If you have questions or would like to discuss the situation, please contact privacy@brunswick.com.

We unreservedly apologise for this unfortunate situation. We highly value our customers, and are committed to protecting your personal information.

Yours sincerely

The C-Map Team

Data Security Measures and Information

Residents of Australia:

Make sure you always exercise good password hygiene. Additional guidance on this from the Australian Cyber Security Centre is available at https://www.cyber.gov.au/protect-yourself);

You will find general information on online safety, cyber security and helpful tips to protect yourself and respond to scams, identity theft and other online risks at https://www.cyber.gov.au/threats.

If you wish to learn more about your rights as a consumer to make a privacy complaint or request, please visit https://www.oaic.gov.au/

Residents of Canada:

We encourage you to exercise good password hygiene and to not reuse passwords on multiple services. We also encourage you to remain vigilant regarding your personal and financial information. If you notice any unusual activity in any of your accounts, please contact your service providers as soon as possible. If you receive any suspicious messages purporting to be from Navico, contact us to confirm its legitimacy.

Additional advice for protecting yourself is available from the Canadian Anti-Fraud Centre at https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm.

Residents of the European Union:

To find general information on cyber security threats in the European Union ("EU") please visit

- https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats;
- https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/nomoreransom
- https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime; and
- https://www.consilium.europa.eu/en/your-online-life-and-the-eu/.

To reduce possible risks, you should be cautious when receiving e-mails or other communications from unknown persons. Additionally, when you receive e-mails from known persons asking you to perform certain actions or provide information, make sure that the e-mail address is correct. If in doubt, call the sender to verify.

It is also strongly recommended to change your passwords that you used so far and that you may have used for several websites, apps or services. For more recommendations on how to manage your

passwords, please see the following guidance from the European Union Agency for Cybersecurity ("ENISA") at https://www.enisa.europa.eu/securesme/cyber-tips/enhance-processes/passwords.

It is also advisable to regularly review your recent bank and credit card statements for any unusual activity. If there are any payments that are not correct, please inform your bank or credit card company immediately. Should this be the case, you should also block or cancel your current credit and bank card and apply for a new one.

Furthermore, there are several online sites offering a free check if your e-mail address has been affected by a data breach, for instance, https://haveibeenpwned.com/.

If you wish to consult your competent data protection supervisory authority ("DPSA"), please find an overview of all DPSA's in the EU at https://edpb.europa.eu/about-edpb/about-edpb/members_en.

Residents of New Zealand

The New Zealand Office of the Privacy Commissioner has been notified of this incident. If you wish to make a complaint to the Privacy Commissioner please visit https://www.privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/ for more information.

You can find general information about online safety, cyber security and helpful tips to protect yourself and respond to scams, identity theft and other online risks at https://www.cert.govt.nz/individuals/.

Residents of Singapore:

To reduce risks, you may wish to adopt the following cyber hygiene measures:

- Change your passwords regularly.
- Avoid using personal information in passwords.
- Use a strong password or passphrase of at least 12 characters which includes upper case, lower case, numbers and/or special characters. To make it easier for you to remember, you can use passphrases by putting together a sentence or combination of words based on a memory unique to you. As passphrases are longer than traditional passwords and tend to be unique, they are more secure than short passwords as it often requires significantly more time for cyber criminals to crack. Avoid using the same password for different accounts.
- Enable two-factor authentication (2FA), where available.
- Ensure that an antivirus software is installed on your device and update it regularly.
- Perform antivirus scans regularly to remove any known malware on your device.
- Enable password protection on data storage devices and lock them up when not in use.
- Limit access to social media accounts. Also, limit sharing of personal information online as threat actors commonly look for and use such personal information to carry out targeted phishing. Review your account privacy settings and permissions and adjust your privacy settings as appropriate.
- Turn on login alerts, if available. The platform should send you an alert when someone logs into your account from an unrecognised device or browser. For email accounts, review any unrecognised login sessions immediately for unusual account activities such as setting of email forwarding rules to unknown accounts.
- Always be wary of suspicious emails and verify before clicking on any links or downloading any attachments, especially if the email came from an unfamiliar sender.
- Verify a link in an email/SMS by checking the domain name of the site, as it is an indicator of whether the site is legitimate. Users can hover their mouse over the link to ensure that they are being directed to the URL stated.

To find out more about how you can protect yourself from a data breach, please visit: www.csa.gov.sg/docs/default-source/publications/singcert/2023/protecting-yourself-from-data-breaches.pdf?sfvrsn=26db3aa0_1.

The Personal Data Protection Commission (PDPC) encourages individuals who have concerns about the ways in which an organisation has handled their personal data to first approach the organisation to clarify the reasons for the organisation's actions and seek an amicable resolution of the matter. Further details, including a template letter for contacting the organisation about your concerns, are available here: https://www.pdpc.gov.sg/Complaints-and-Reviews/Report-a-Personal-Data-Protection-Concern.

Should you wish to submit a personal data protection complaint to the PDPC, you may do so via this link: https://www.pdpc.gov.sg/complaints-and-reviews/report-a-personal-data-protection-concern/personal-data-protection-complaint.

General information about cyber security and data security measures that organisations who handle your personal data should adopt is available at https://www.pdpc.gov.sg/. Resources tailored for you as an individual can be found at https://www.pdpc.gov.sg/Individual.

Residents of the United States of America:

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111.
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742.
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), http://www.ftc.gov/idtheft .

If you are a resident of California, Connecticut, Iowa, Maryland, Massachusetts, New York, North Carolina, Oregon, Puerto Rico, Rhode Island, or Washington, D.C., you may contact and obtain information from your state Attorney General at the following:

- California Department of Justice, Office of Privacy Protection, PO Box 944255, Sacramento, CA 94244-2550, 1-800-952-5225, www.oag.ca.gov/privacy.
- Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

- Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut St., Des Moines, IA 50319, 1-515-281-5164, https://www.iowaattorneygeneral.gov/.
- Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 or 1-410-576-6300, www.marylandattorneygeneral.gov.
- Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.
- New York Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.
- North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, https://ncdoj.gov/, 1-919-716-6400 or 1-877-566-7226.
- Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-503-378-4400, https://www.doj.state.or.us/.
- The Puerto Rico Department of Justice, Calle Teniente César González 677 Esq. Ave. Jesús T. Piñero, San Juan, Puerto Rico, 787-721-2900, http://www.justicia.pr.gov/.
- 787-722-7555 or https://www.daco.pr.gov/servicios/querellas/.
- Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, https://riag.ri.gov/, 1-401-274-4400.
- Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, (202) 727-3400, www.oag.dc.gov.

If you are a resident of Massachusetts or Rhode Island, please note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Note: The delivery of this notice has not been delayed as a result of a law enforcement investigation.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a personal identification number ("PIN") that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information: (i) Your full name (including middle initial as well as Jr., Sr., II, III, etc.), (ii) Social Security number, (iii) Date of birth, (iv) If you have moved in the past five years, provide the addresses where you have lived over the prior five years, (v) Proof of current address such as a current utility bill or telephone bill, (vi) A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.), (vii) If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (“PIN”) or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

* * * * * * * * * *

Skip to Help & Support

- About C-MAP
- Copyright Acknowledgement
- Notices and Warnings
- C-Map Data License Agreement ("EULA")
- Terms of Use
- Privacy Policy
- Cookie Policy

Help & Support

Skip to Be the first to receive the latest news and product updates

- Knowledge Base
- Compatibility List
- Dealer Locator
- Contact Us
- Chart Features

Be the first to receive the latest news and product updates

Your personal details are safe with us. For more info, read our Privacy Policy.

Follow us