



Matthew Toldero, Partner
Cybersecurity & Data Privacy Team
One West 4th Street, Suite 850
Winston-Salem, NC 27101
mtoldero@constangy.com

Mobile: 336.448.8552
Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

January 2, 2025

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: **Notice of Data Security Incident**

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Army Navy Country Club (“ANCC”), a private country club located in Virginia, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ANCC does not waive any rights or defenses regarding the applicability of Virginia law, the applicability of the Virginia data event notification statute, or personal jurisdiction

1. Nature of the Security Incident

On October 8, 2024, ANCC became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, ANCC immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. Through the investigation, it was revealed that certain information was acquired without authorization on or about October 6, 2024. Following this confirmation, ANCC commenced a comprehensive review of the potentially affected data and on November 21, 2024, ANCC determined that personal information belonging to certain current and former employees may have been impacted in connection with this incident. ANCC then worked diligently to obtain contact information to effectuate notification to potentially affected individuals. This process was completed on November 29, 2024.

Please note that ANCC has no current evidence to suggest misuse or attempted misuse of personal information involved.

2. Number of Affected Maryland Residents & Information Involved

On January 2, 2025, ANCC notified one hundred and fifty (150) Maryland residents. The information involved included name, address, and Social Security number. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

3. Steps Taken to Address the Incident

In response to the incident, ANCC retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. ANCC also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

Further, while ANCC is not aware of misuse of any information as a result of this incident, out of an abundance of caution, ANCC is providing individuals with information about steps that they can take to help protect their personal information. Additionally, the notification letters provide 12 months of complimentary identity protection services to each individual whose personal information was potentially affected by this event, including credit and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Those services are offered by IDX, a company specializing in fraud assistance and remediation services. IDX will also support a call center for ninety (90) days to answer questions and assist with enrollment. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

ANCC notified federal law enforcement and is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

4. Contact Information

ANCC remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at mtoldero@constangy.com or 336.448.8552.

Sincerely,



Matthew Toldero
Partner, Cybersecurity & Data Privacy
Team

Enclosed: Consumer Notification Letter



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

January 2, 2025

Re: Notice of Data <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident experienced by Army Navy Country Club (“ANCC”) that may have involved your personal information. At ANCC, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On October 8, 2024, ANCC discovered a network disruption and immediately initiated an investigation of the matter. We engaged cybersecurity experts to assist with the process. As a result of the investigation, we determined that a limited number of files may have been accessed or acquired without authorization. ANCC then undertook a comprehensive review of affected files and, on or about November 21, 2024, learned that personal information associated with certain current and former employees was contained within the potentially affected data. We then worked diligently to obtain missing address information to effectuate notification to affected individuals, which was completed on November 29, 2024. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved? The information potentially impacted may have included your name, address, and Social Security number.

What We Are Doing. As soon as ANCC discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. ANCC also notified the Federal Bureau of Investigation and will cooperate with any resulting investigation.

Additionally, we are offering you the opportunity to enroll in credit monitoring and identity protection services through IDX at no cost to you. The IDX services, which are free to you upon enrollment, include <<12/24 months>> of credit monitoring and CyberScan dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you to resolve issues if your identity is compromised.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through IDX at no cost to you. To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

You can enroll in the IDX identity protection services by calling (833) 903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. Please note the deadline to enroll is April 2, 2025.

For More Information. If you have questions, please call IDX at (833) 903-3648, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Patrick S. King, CCM, CCE
General Manager / Chief Operating Officer

Army Navy Country Club
1700 Army Navy Drive
Arlington, VA 22202

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC):

600 Pennsylvania Ave, NW, Washington, DC 20580; consumer.ftc.gov, and www.ftc.gov/idtheft; 1-877-438-4338

Virginia Attorney General

202 North Ninth Street
Richmond, VA 23219
oag.state.va.us
1-804-786-2042

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

The Capitol
New York, NY 12224
ag.ny.gov
1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
riag.ri.gov
1-401-274-4400
RI individuals notified:

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
dos.ny.gov/consumerprotection
1-212-416-8433

California Attorney General

1300 I Street
Sacramento, CA 95814
oag.ca.gov/privacy
800-952-5225

Oregon Attorney General

1162 Court Street NE
Salem, OR 97301
doj.state.or.us/consumer-protection
877-877-9392

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.