



Jason Cherry, Esq.  
2029 Century Park East  
Suite 1100  
Los Angeles, CA 90067  
jcherry@constangy.com  
Tel.: 207.745.1397

December 21, 2023

Attorney General Anthony G. Brown  
Office of the Attorney General  
St. Paul Plaza  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
Email: [IDtheft@oag.state.md.us](mailto:IDtheft@oag.state.md.us)

Dear Attorney General Brown:

Constangy, Brooks, Smith and Prophete LLP (“Constangy”) represents Colony Family Offices, LLC. (“Colony”) in connection with an incident described in greater detail below.

### **1. Nature of Incident**

On September 3, 2023, Colony’s security team detected an unusual sign-in on an employee account. After detecting and promptly containing the incident, Colony launched an investigation with the support of external cybersecurity experts to learn more about the scope of the incident and any impact to data. Through that investigation, Colony learned of information suggesting that an unknown actor gained unauthorized access to data and potentially acquired certain files, some of which may have contained personal information. Colony reviewed the files in detail, and on or about November 20, 2023, Colony determined that certain information was potentially impacted.

The potentially impacted information included names and a mixture of variable categories of personal information, as defined by state law: Social Security numbers, full driver’s license numbers, passport numbers, and financial account numbers with no PIN, password, or other means to access the account.

### **2. Number of Maryland Residents affected**

Colony notified five residents of Maryland of the incident via first class U.S. mail on December 21, 2023. A sample copy of the notification letter is included with this correspondence.

### **3. Steps taken relating to the incident**

Upon discovering the issue, Colony took the steps described above. Colony has also provided notice of the incident to potentially impacted individuals on December 21, 2023.

In addition, Colony is offering affected individuals complimentary credit monitoring and identity protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring,

a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help them resolve issues if their identity is affected.

#### **4. Contact information**

If you have any questions or need additional information, please do not hesitate to contact me at 207.745.1397 or [jcherry@constangy.com](mailto:jcherry@constangy.com).

Very truly yours,



Jason Cherry

Encl.: Sample Consumer Notification Letter



Return to IDX  
4145 SW Watson Ave.  
Suite 400  
Beaverton, OR 97005

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

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

December 21, 2023

**Re: Notice of Data** <<Variable Text 1 – Subject Line>>

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

We are writing to inform you of an incident recently experienced by Colony Family Offices, LLC. (“Colony”) which may have affected the security of some of your personal information. Please review this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

**What Happened.** On December 11, 2023, our investigation revealed that your personal information may have been accessed without authorization. The investigation stems from a potential data security incident that occurred on or about September 3, 2023, when we identified suspicious activity associated with one employee email account. We promptly launched an investigation into the nature and scope of this incident and took steps to secure our email environment. With the assistance of an independent cybersecurity forensics firm, we learned that an unauthorized individual accessed the account. Although there was no conclusive evidence of data loss, the protection of data in our possession is one of our highest priorities.

**What Information Was Involved.** The information potentially impacted by this incident may have included your name and Social Security number, driver license number, or a financial account number with no PIN, password, or other means of accessing the account. **Please note that Colony has no evidence of the misuse or attempted misuse of any information potentially affected by this incident.**

**What We Are Doing.** As soon as we discovered the incident, we took the steps described above. In addition, we have implemented measures to further enhance the security of our email environment in order to minimize the risk of a similar incident from occurring in the future. We are also providing you with information about steps you can take to help protect your personal information.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you 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. We also encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Standard Time. Please note the deadline to enroll is <<Date>>.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

**For More Information.** Please call IDX at 1-800-939-4170 for any additional questions you may have. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Sincerely,



Eric Ridenour  
**Colony Family Offices**  
4250 Congress Street, Suite 175  
Charlotte, NC 28209

(Enclosure)

## ADDITIONAL STEPS YOU CAN TAKE TO FURTHER 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). 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 Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.consumer.ftc.gov](http://www.consumer.ftc.gov), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

**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 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 can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, [www.equifax.com](http://www.equifax.com).
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com).
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, [www.transunion.com](http://www.transunion.com).

**Fraud Alerts:** There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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>. Military members may also place an Active-Duty Military Fraud Alert on their credit reports while deployed. An Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

**Credit or Security Freezes:** Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

**IRS Identity Protection PIN:** You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit [http://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).

**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.

**Additional information:**

**District of Columbia:** The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [oag@dc.gov](mailto:oag@dc.gov)

**California:** California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

**Massachusetts:** Massachusetts Attorney General can be reached at: 1 Ashburton PI Boston, MA 02108; 617-727-8400; <https://www.mass.gov/orgs/office-of-the-attorney-general>

**Maine:** Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

**Maryland:** Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; [oag@state.md.us](mailto:oag@state.md.us) or [IDTheft@oag.state.md.us](mailto:IDTheft@oag.state.md.us)

**North Carolina:** North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; [www.ncdoj.gov](http://www.ncdoj.gov)

**New York:** New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

**Rhode Island:** Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>.

**Texas:** Texas Attorney General can be reached at: 300 W. 15<sup>th</sup> Street, Austin, Texas 78701; 800-621-0508; [texasattorneygeneral.gov/consumer-protection/](http://texasattorneygeneral.gov/consumer-protection/)

**Vermont:** Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; [ago.info@vermont.gov](mailto:ago.info@vermont.gov)