



Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
aweaver@constangy.com
Mobile: 941.875.5335

August 26, 2026

VIA ONLINE SUBMISSION

Attorney General Nick Brown
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
Email: SecurityBreach@atg.wa.gov

RE: Notice of Data Security Incident

To Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Cascade Coffee, LLC, in connection with a data security incident described below. Cascade is providing notice to potentially affected individuals of the incident. The purpose of this letter is to provide notice to your office pursuant to RCW § 19.255.010.

I. NATURE OF THE SECURITY INCIDENT

Cascade learned of unusual activity involving its network environment on July 30th, 2026. Cascade promptly initiated an investigation of the matter with the assistance of cybersecurity experts. This investigation determined that certain files and folders containing information pertaining to Cascade employees may have been accessed or downloaded without authorization in connection with the incident.

II. NUMBER OF WASHINGTON RESIDENTS AFFECTED

Cascade provided notification to 610 Washington residents on August 24, 2026, via First-Class U.S. Mail. A sample copy of the notification letter is included with this correspondence.

The potentially affected data elements included names, dates of birth, Social Security numbers, and/or other information associated with individuals' employment with Cascade.

III. ACTIONS TAKEN IN RESPONSE TO THE INCIDENT

Once Cascade became aware of the unusual activity, it took steps to further secure its environment and launched a comprehensive investigation. Cascade thereafter worked

Attorney General Nick Brown
August 26, 2026

Constangy, Brooks, Smith & Prophete, LLP

diligently to determine what information may have been affected and the individuals to whom the information pertained, and moved swiftly to provide notice to those individuals.

Cascade has established a toll-free call center through Cyberscout, a TransUnion company, to answer questions about the incident and address related concerns. In addition, Cascade is offering Washington residents twelve (12) months of complimentary credit and identity protection services through Cyberscout.

IV. CONTACT INFORMATION

If you have any questions or need additional information, please do not hesitate to contact me at 215.770.4234 or aweaver@constangy.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Aubrey Weaver', with a stylized, cursive script.

Aubrey Weaver
Constangy, Brooks, Smith & Prophete, LLP

Encl. Sample Notification Letter

Cascade Coffee, LLC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057

CASCADE
-COFFEE-



August 24, 2026

Subject: Notice of Data Security Incident

Dear [REDACTED]:

We are writing regarding a recent data security incident that may have involved your personal information. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened?

On July 30th, 2026, we identified suspicious activity associated with our network. As soon as we became aware of the activity, we promptly initiated our incident response protocols, took steps to secure our systems, and engaged cybersecurity experts to assist with the investigation. The investigation determined that an unauthorized actor may have accessed or downloaded certain files and folders where your personal information was stored. We now know that this unauthorized activity took place early in the morning on July 30th.

What Information Was Involved?

The personal information that may have been involved includes your name, date of birth, Social Security number, and/or other information associated with your employment.

What We Are Doing.

We take the confidentiality, privacy, and security of Cascade's and our employees' data seriously. We are working with a team of experts to investigate this matter and to implement additional safeguards in our systems. We are also reviewing and updating our policies and procedures relating to data privacy and security consistent with those efforts.

What You Can Do.

We encourage you to review the information provided with this letter for measures you can take to help protect your personal information.

Additionally, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you on the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted, please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and email account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information.

If you have any questions, a dedicated support center has been established. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding major U.S. holidays. Please call the help line at **1-800-405-[REDACTED]** and supply the fraud specialist with your unique code listed above.

Your confidence and trust are important to us. We regret that this occurred and apologize for any inconvenience this incident may have caused.

Sincerely,

John Gilbert, CEO
Cascade Coffee, LLC
1525 75th Street, SW, #100
Everett, WA 98203

Steps You Can Take to Help Protect Your Personal 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 (the "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 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 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 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov 877-438-4338	California Attorney General 1300 I Street Sacramento, CA 95814 www.oag.ca.gov/privacy 800-952-5225
Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 www.marylandattorneygeneral.gov/Pages/CPD 888-743-0023	Oregon Attorney General 1162 Court St., NE Salem, OR 97301 www.doj.state.or.us/consumer-protection 877-877-9392

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification 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. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.