



Robert F. Walker
1020 Highland Colony Parkway, Suite 310
Ridgeland, Mississippi 39157
Robert.F.Walker@lewisbrisbois.com
Direct: 601.499.8126

October 15, 2025

RECEIVED

OCT 21 2025

CONSUMER PROTECTION

Via First-Class Mail:

Attorney General John Formella
Consumer Protection Bureau
Office of the Attorney General
1 Granite Place South
Concord, NH 03301

Re: Our Client : The Branch Group, Inc.
Matter : Data Security Incident
LBBS File No. : 49975.62

Dear Attorney General Formella:

We are writing on behalf of The Branch Group, Inc. ("The Branch Group") with respect to a data security incident described in more detail below. The Branch Group takes the security and privacy of the information in its control seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of New Hampshire resident(s) potentially affected, what information has been compromised, and the steps taken in response to the incident. We have also enclosed hereto samples of the notifications made to the potentially impacted individuals, which include an offer of free credit monitoring.

1. Nature of the Security Incident

On or about January 14, 2025, The Branch Group became alerted to a cybersecurity incident. Upon discovering the incident, The Branch Group immediately took steps to secure the network environment and engaged cybersecurity experts to conduct an investigation.

The forensic investigation determined that certain files may have been acquired without authorization. After a comprehensive review of the data potentially impacted in the incident, which

concluded on October 1, 2025, it was determined that certain personally identifiable information was potentially impacted as a result of the incident. The Branch Group then took steps to notify potentially impacted individuals as quickly as possible.

As of this writing, The Branch Group has not received any reports of misuse of information and/or related identity theft since the date of incident.

2. Number of New Hampshire Residents Affected

A total of one (1) resident of New Hampshire was potentially affected by this incident. A notification letter was mailed to the potentially impacted individual on October 15, 2025, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon detecting the incident, The Branch Group moved quickly to initiate a response, which included conducting an investigation with the assistance of forensic specialist and confirming the security of its network through global password resets, implementing multifactor authentication, wiping and rebuilding affected systems, reviewing and revising policies, and taking steps to mitigate potential harm.

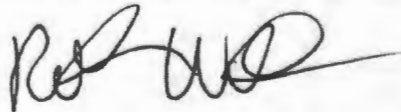
The Branch Group has extended to the potentially impacted individuals an offer for free credit monitoring and identity theft protection through CyberScout, a TransUnion company. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

4. Contact Information

The Branch Group remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Robert.F.Walker@lewisbrisbois.com or 601.499.8126.

Very truly yours,

Lewis Brisbois Bisgaard & Smith, LLP



Robert F. Walker, Esq.

October 15, 2025
Page 3

cc: Lewis Brisbois LLP
Attn: Sarah Cobble, Esq.

Enclosures: *Sample Notification Letter*

The Branch Group, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1548



5_0000760



[REDACTED]
[REDACTED]
[REDACTED]

October 15, 2025

Notice of Data Security Incident

Dear [REDACTED],

You are receiving this letter because you are an employee of The Branch Group, Inc. We are writing to inform you of an incident that may have exposed your personal information. We take the security of your personal information seriously and want to provide you with information and resources that you can use to protect your information going forward.

What Happened:

On or about January 14, 2025, we detected a network security incident, in which an unauthorized third-party attempted to access our network environment. We immediately engaged third-party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. Our investigation, which concluded on August 22, 2025, determined an unauthorized third party acquired certain individual personal information during this incident. A thorough review of the impacted data determined that some of your personal information was present in the impacted data set. We then took steps to notify you of the incident as quickly as possible.

What Information Was Involved:

We found no evidence that your information has been specifically misused; however, it is possible that the following personal information could have been accessed by an unauthorized third party: first and last name, Social Security number, Driver's License number, government identification number, passport number, payment card number and expiration date, card verification value code, and security code. **Notably, the types of information affected may be different for each individual, and not every individual had all of the above listed elements exposed.**

What We Are Doing:

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate a response, which included conducting an investigation with the assistance of forensic specialists and confirming the security of our network environment. We wiped and rebuilt affected systems and have taken steps to bolster our network security. We are also reviewing and altering our policies, procedures, and network security software relating to the security of our systems and servers, as well as how we store and manage data.

Additionally, **while we have no evidence that your information has been misused**, 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 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you 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 event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

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 e-mail account and may not be available to minors under the age of 18. Please note 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:

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 holidays. Please call the help line at 1-833-378-0170 and be prepared to supply the fraud specialist with your unique code listed above. You are encouraged to take full advantage of these services.

Enclosed you will find additional materials regarding the resources available to you, and the steps you can take to further protect your personal information.

Again, we value the security of your personal data and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

The Branch Group, Inc.



Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, it is required by state law that you are informed of your right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. There are approximately 2 Rhode Island residents that may be impacted by this event.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).