



BNBuilders
Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Notice of Data Breach

Dear <<Full Name>>,

We are writing to notify you that BNBuilders (“BNB”) experienced a data security incident that may have involved your personal information. In this letter, we describe what happened, how we are handling the Incident, what you can do, and who you can contact with questions.

What Happened

On July 24, 2024, BNB learned that it was the victim of a data security incident (the “Incident”). With assistance from third-party experts, we took immediate steps to secure our systems and investigate the nature and scope of the Incident. Based on our investigation, the incident appears to have occurred between July 17, 2024 and July 24, 2024.

We conducted an extensive investigation and worked diligently to determine whether any personally identifiable information may have been subject to unauthorized access or acquisition during the Incident.

What Information Was Involved

After reviewing available information, we concluded the Incident may have impacted certain personally identifiable information that we maintain consisting of your name, <<breached elements>>.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice so you can take steps to minimize any risk that your information will be misused. We also notified law enforcement of the Incident.

We apologize for any concern this Incident may cause you. BNB recognizes the importance of safeguarding your personal information and we endeavor to implement reasonable and appropriate safeguards to do so.

As part of our ongoing focus on cybersecurity, we have augmented our security practices to minimize the risk of a similar incident occurring in the future. At the end of this letter, we have included precautionary steps you can take to safeguard your personal information as well as resources where you can find additional information.

As an added precaution, we are offering you a chance to enroll in complimentary access to Experian IdentityWorksSM for 12 months.

- If you believe there was fraudulent use of your information as a result of this Incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the Incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).
- Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.
- While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:
 - Ensure that you **enroll by <<Enrollment Deadline>>**, no later than 5:59 pm CT (Your code will not work after this date.)
 - **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
 - Provide your **activation code: <<Activation Code>>**
- If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057 by <<Enrollment Deadline>>, no later than 5:59pm CT. Be prepared to provide engagement number <<Engagement #>> as proof of eligibility for the Identity Restoration services by Experian.
- A credit card is not required to enroll in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:
 - **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
 - **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
 - **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
 - **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
 - **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- When enrolling, you will need to reference the enrollment code, so do not discard this letter.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

What You Can Do

In addition to enrolling in the complimentary credit and identity monitoring services discussed above, consider taking some of the steps on the attached informational sheet, as you deem necessary.

For More Information

If you have questions or concerns, please contact us at 855-277-8095.

We apologize for any concern or inconvenience this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rich Finlay". The signature is written in a cursive style with a large initial "R" and a long, sweeping tail.

Rich Finlay
CFO
BNBuilders

Protecting Your Personal Information

As with any data incident, we recommend that you remain vigilant. The following information includes steps to minimize risk that your personal information will be misused and additional resources for more information.

1. Contact the three major credit-reporting agencies as soon as possible to:

- Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed and your request will be shared with the other two agencies. 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. This fraud alert will remain on your credit file for one year.
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

<u>Equifax</u> P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285
<u>Experian</u> P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742
<u>TransUnion</u> Fraud Victim Assistance Dept. P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

2. You can also request information from these agencies about identity theft and place a “security freeze” on your credit accounts. To place a security freeze, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies’ online security freeze request procedures.

<u>Equifax Security Freeze</u> 1-888-298-0045 www.equifax.com P.O. Box 105788 Atlanta, GA 30348
<u>Experian Security Freeze</u> 1-888-397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013
<u>Trans Union Security Freeze</u> 1-888-909-8872 www.transunion.com P.O. Box 160 Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you have one.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

3. Review bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
4. The Fair Credit Reporting Act (FCRA) establishes procedures for correcting mistakes on your credit record and requires that your record be made available only for certain legitimate business needs. Under the FCRA, both the credit bureau and the organization that provided the information to the credit bureau (the "information provider"), such as a bank or credit card company, are responsible for correcting inaccurate or incomplete information in your report. To protect your rights under the law, contact both the credit bureau and the information provider.
5. If you suspect or know that you are the victim of identity theft, contact local law enforcement or the office of your state Attorney General. You can also contact the Federal Trade Commission's Fraud Department which will collect all information and make it available to law enforcement agencies.

The Federal Trade Commission also offers consumer assistance and educational materials on identity theft and privacy issues. You can contact the FTC through the website, phone number or mailing address below:

www.ftc.gov, www.consumer.gov/idtheft
(877) 438-4338.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

6. In addition to the FTC, you can obtain information on identity theft from your state Office of the Attorney General.

California Residents: You can obtain additional information about identity theft from the Office of the Attorney General at [Identity Theft | State of California - Department of Justice - Office of the Attorney General](#).

New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.

North Carolina Residents: You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

Oregon Residents: You can obtain additional information from the Oregon DOJ Consumer Protection Office at [Identity Theft - Oregon Department of Justice : Consumer Protection \(state.or.us\)](#).