



LEWIS BRISBOIS BISGAARD & SMITH LLP

Kevin W. Yoegel  
550 E. Swedesford Road, Suite 270  
Wayne, Pennsylvania 19087  
Kevin.Yoegel@lewisbrisbois.com  
Direct: 215.253.4255

June 24, 2021

**VIA ELECTRONIC MAIL**

Attorney General Gordon J. MacDonald  
Office of the Attorney General  
New Hampshire Department of Justice  
33 Capitol Street  
Concord, NH 03301  
Email: attorneygeneral@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Brady Sullivan Properties (“BSP”), a real estate development company located in New Hampshire, in connection with a data security incident described in greater detail below. BSP takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

**1. Nature of the security incident.**

In December 2020, BSP learned of unusual activity involving an employee email account. Upon discovering this activity, BSP immediately began an investigation and took steps to secure the affected account. BSP also engaged an independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation concluded that the one employee email account may have been accessed without authorization. BSP then undertook a diligent search of the affected account’s contents to identify any personal information that may have been contained therein and took steps to gather contact information for the potentially affected individuals. These processes were completed on June 10, 2021.

On June 23, 2021, BSP identified 562 New Hampshire residents whose information was contained within the affected email account. The potentially affected information includes the New Hampshire residents’ names, Social Security numbers, driver's license or state identification card numbers, other government identification numbers, and/or credit or debit card information.

**2. Number of New Hampshire residents affected.**

BSP is preparing to issue notification letters to the 562 New Hampshire residents regarding this data security incident via first-class U.S. mail on June 24, 2021. A sample copy of the notification letter is attached hereto.

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

BSP has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps have included working with leading cybersecurity experts to further enhance the security of its email platform by implementing multi-factor authentication and disabling legacy email protocols within the environment. Out of an abundance of caution, BSP is also offering the potentially affected individuals complimentary credit monitoring, identity protection services, and identity theft insurance at no cost through IDX.

**4. Contact information.**

BSP remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (215) 253-4255 or via email at [Kevin.Yoegel@lewisbrisbois.com](mailto:Kevin.Yoegel@lewisbrisbois.com).

Regards,



Kevin W. Yoegel of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

KWY:ALW

Attachment: Consumer Notification Letter Template

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

To Enroll, Please Call:  
1-833-903-3648  
Or Visit:  
<https://app.idx.us/account-creation/protect>  
Enrollment Code: <<XXXXXXXXXX>>

June 24, 2021

Subject: Notice of Data Security Incident

Dear <<First Name>> << Last Name>>:

I am writing to inform you of a data security incident that may have affected your personal information. At Brady Sullivan Properties (“BSP”), we take the privacy and security of personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to help protect your information, including by enrolling in the complimentary identity protection services we are making available to you.

**What Happened?** In December 2020, BSP learned of unusual activity involving a BSP email account. Upon discovering this activity, we immediately began an investigation and took steps to secure the email account. We also engaged an independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation concluded that the email account may have been accessed without authorization between December 9 and December 10, 2020. BSP then conducted a comprehensive review of the affected account’s contents and took steps to gather contact information need to notify all potentially affected individuals. We completed this on June 10, 2021, and determined that some of your information was contained within the email account.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other BSP information systems. We are not aware of the misuse of any personal information that may have been involved in this incident.

**What Information Was Involved?** The potentially affected information may have included your <<variable 1>>.

**What Are We Doing?** As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our email environment and to reduce the risk of a similar incident occurring in the future, including through the implementation of multi-factor authentication.

In addition, we are providing you with information about steps you can take to help protect your personal information and, out of an abundance of caution, we are offering you credit monitoring and identity theft restoration services at no cost to you through IDX, a leader in risk mitigation and response. These services include <<variable 2>> credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery services. With this protection, IDX will help you to resolve issues if your identity is compromised.

To receive the IDX services, you must be over the age of 18, have established credit in the United States, have a Social Security number issued in your name, and have a United States residential address associated with your credit file. Please note that the deadline to enroll in the IDX services is September 24, 2021.

**What Can You Do?** We recommend that you review the guidance included with this letter about how to help protect your information. You can also contact IDX with any questions and to enroll in the free IDX services by calling

1-833-903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available to assist you Monday through Friday from 9:00 am – 9:00 pm Eastern Standard Time.

We encourage you to take full advantage of this service offering. IDX representatives are fully versed on the incident and can answer questions or respond to concerns you may have. More information is enclosed with this letter.

**For More Information:** Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call our dedicated call center at 1-833-903-3648 Monday through Friday from 9:00 am – 9:00 pm Eastern Standard Time.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

*Megan Hilson*

Megan Hilson  
General Counsel  
Brady Sullivan Properties

## 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 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](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 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>.

**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.

**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](http://consumer.ftc.gov), and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
[oag.state.md.us](http://oag.state.md.us)  
1-888-743-0023

**New York Attorney General**

Bureau of Internet and Technology  
Resources  
28 Liberty Street  
New York, NY 10005  
1-212-416-8433

**North Carolina Attorney General**

9001 Mail Service Center  
Raleigh, NC 27699  
[ncdoj.gov](http://ncdoj.gov)  
1-877-566-7226

**Rhode Island Attorney General**

150 South Main Street  
Providence, RI 02903  
<http://www.riag.ri.gov>  
1-401-274-4400

**Washington D.C. Attorney General**

441 4th Street, NW  
Washington, DC 20001  
[oag.dc.gov](http://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>.

**Personal Information of a Minor:** You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies may be found above.



## Enrollment in IDX Identity Protection

**Website and Enrollment.** Please visit <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code included with this letter.

**Activate the credit monitoring** provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**Telephone.** Contact IDX at 1-833-903-3648 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**This IDX enrollment will include <<variable 2>> enrollment into:**

**SINGLE BUREAU CREDIT MONITORING** - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

**CYBERSCAN™** - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

**IDENTITY THEFT INSURANCE** - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

**FULLY-MANAGED IDENTITY RECOVERY** - IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDX Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.