Melissa K. Ventrone
T (312) 360-2506
Email:mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

May 2, 2025

VIA PORTAL SUBMISSION

Nebraska Attorney General
2115 State Capitol
Lincoln, NE 68509

Re: Data Security Incident

Dear Attorney General Hilgers:

We represent Deed Research, Inc. ("Deed Research") with respect to a data security incident involving personal information described below. Deed Research takes the security of the information in its control seriously and is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

1. Nature of security incident.

On January 25th, 2025, Deed Research identified suspicious activity on its servers. They immediately implemented their incident response protocols and independent computer forensic specialists were engaged to help investigate the incident. The investigation found that some documents were taken from Deed Research's system. The affected documents were reviewed, and on April 2, 2025, Deed Research learned that some personal information may have been impacted, including names, and some combination of the following: Social Security numbers and financial account information.

2. Number of residents affected.

627 Nebraska residents were notified of the incident. A notification letter was sent to the potentially affected individuals on May 2, 2025. A copy of the form notification letter is enclosed as Exhibit A.

3. Steps taken in response to the incident.

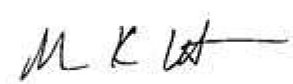
Since the incident, Deed Research Tech has taken steps to prevent a similar incident in the future, including performing a global password resent, deploying endpoint detection monitoring software on all systems, and implementing additional security controls. Additionally, letters were mailed to potentially affected individuals, which included instructions for enrolling in 12 months of credit monitoring and identity protection services through Cyberscout through Identity Force, a TransUnion company, at no cost.

4. Contact Information

Deed Research takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL



Melissa K. Ventrone
Member

Deed Research, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

EXHIBIT A

P
[redacted] NE [redacted]

000010102G0400

P

May 2, 2025

Re: Notice of Data

Dear [redacted],

Deed Research, Inc. provides back-office support for a limited number of title and escrow companies located in the Midwest. We are writing to let you know about a data security incident that may have impacted some of your personal information. We may have your information if you currently or previously worked for Deed Research or one of our related companies. We take the privacy and security of your information seriously and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

On January 25th, 2025, we identified suspicious activity on our servers. We immediately implemented our incident response protocols and independent computer forensic specialists were engaged to help investigate the incident. The investigation found that some documents were taken from our system. The affected documents were reviewed, and on April 2, 2025, we learned that some of your personal information may have been impacted.

What Information Was Involved?

Information potentially impacted may include your name, Social Security Number; Date of Birth; Financial Account Number; Driver's License or State ID. We have no evidence that your information has been misused, however, we wanted to make you aware of the incident out of an abundance of caution.

What We Are Doing:

We have taken steps to prevent this kind of event in the future, such as changing passwords, deploying endpoint detection and monitoring tools, and implementing other security controls. We are also cooperating with law enforcement.

In addition, although there is no evidence your information was 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.

How do I enroll for the free 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 e-mail 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.

What You Can Do:

You should remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity over the next 12 months. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit. We also encourage you to take full advantage of this service offering.

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 1-833-998-8174 and supply the fraud specialist with your unique code listed above.

For More Information:

If you have questions, please call 1-833-998-8174, Monday through Friday from 8 a.m. to 8 p.m. Eastern Time, excluding major US holidays. Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you.

Sincerely,

Deed Research, Inc.

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to **https://bfs.cyberscout.com/activate** and follow the instructions using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your Cyberscout identity protection 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.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

0000102028000 P

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a violator. 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. You can 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.

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; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of [XX] Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.