



October 27, 2023

**Anjali C. Das**  
312.821.6164 (Direct)  
[anjali.das@wilsonelser.com](mailto:anjali.das@wilsonelser.com)

**Via E-Mail: [Idtheft@oag.state.md.us](mailto:Idtheft@oag.state.md.us)**

Attorney General Anthony Brown  
Office of the Attorney General  
Identity Theft Unit  
200 St. Paul Place  
Baltimore, MD 21202

**Re: Notice of Data Security Incident**

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker, LLP (“Wilson Elser”) represents The McKnight Group, a an architecture and design agency based in Grove City, Ohio, with respect to a cybersecurity incident that was discovered by The McKnight Group on April 17, 2023 (hereinafter, the “Incident”). Please note The McKnight Group takes the security and privacy of the information within its control seriously, and has taken steps to prevent a similar incident from occurring in the future. This letter will serve as a notice of the Incident and to inform you of the steps The McKnight Group has taken in response to the Incident.

**1. Nature of the Incident**

On April 17, 2023, The McKnight Group was notified as to potential unauthorized activity within its computer network. Upon discovery of the Incident, The McKnight Group engaged a specialized incident response vendor to secure its network and conduct a thorough forensic investigation to determine the nature and scope of the unauthorized activity. The findings from the forensic investigation indicated that unauthorized activity occurred within The McKnight Group’s network for a period of time starting on April 14, 2023, until April 15, 2023.

The McKnight Group worked diligently with a data mining firm to determine what information was maintained within the compromised systems for purposes of providing this notice of the incident to the affected individuals. Based upon the results of its review, The McKnight Group determined that the following elements of personal information may have been accessed and/or acquired by an unauthorized individual: names, addresses, dates of birth, payment card numbers and access information, financial account numbers and access information, drivers’ license numbers, and Social Security numbers. The specific data elements that were impacted vary per individual.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky  
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Missouri • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix  
San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

**wilsonelser.com**

As of this writing, The McKnight Group has not received any reports of related identity theft, since the date of the Incident to the present.

**2. Number of Maryland residents affected.**

The McKnight Group discovered that the Incident may have resulted in unauthorized exposure of information pertaining to one (1) Maryland resident. A notification letter to the individual was mailed on October 27, 2023, by First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

**3. Steps taken in response to the Incident.**

The McKnight Group is committed to ensuring the security and privacy of all personal information within its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, The McKnight Group notified law enforcement and engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, North Lawndale has taken steps to strengthen its security posture to prevent a similar event from occurring again in the future.

The McKnight Group is also offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through TransUnion to potentially affected individuals residing in Maryland to help protect their identity. Additionally, The McKnight Group provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies and Federal Trade Commission, information on how to obtain a free credit report, and a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports.

**4. Contact Information**

The McKnight Group remains dedicated to protecting the sensitive information within its control. Should you have any questions or need additional information, please do not hesitate to contact me at [anjali.das@wilsonelser.com](mailto:anjali.das@wilsonelser.com) or 312.821.6164.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**



Anjali C. Das

# **EXHIBIT A**

McKnight Development  
c/o Cyberscout  
1 Keystone Ave Unit 700  
Cherry Hill, NJ 08003  
DB08014



[REDACTED]

October 27, 2023

### Notice of Data Breach

Dear [REDACTED]:

We are reaching out to let you know The McKnight Group recently experienced a data security incident which may have affected your personal information. Please note we take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to safeguard your information.

### What Happened

On April 17, 2023, The McKnight Group detected unauthorized activity within its network ("Incident"). Upon discovery of this Incident, The McKnight Group promptly engaged a specialized cybersecurity firm to secure its environment and conduct an investigation to determine the nature and scope of the Incident. The findings from the forensic investigation indicated that its current and former employees' personally identifiable information may have been accessed by an unauthorized user. Based on the results of the forensic investigation, The McKnight Group worked diligently with a data mining firm to determine what information was maintained within the compromised systems for purposes of providing this notice of the incident to the affected individuals.

### What Information Was Involved

The elements of your personal information that may have been exposed included, and potentially were not limited to your: name, address, Date of Birth, Social Security Number, US Drivers License Number.

Please note that at this time we have received no evidence indicating that any employee information has been misused as a result of this Incident.

### What We Are Doing

The McKnight Group takes the privacy and security of the personal information within its control very seriously and continues to investigate and closely monitor the situation. Further, have taken steps to strengthen our security posture to prevent a similar event from occurring again in the future.

In addition, in order to address any individual concerns and mitigate any exposure or risk of harm following this Incident, 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 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 through Identity Force, 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://secure.identityforce.com/benefit/mcknightd> 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 ninety (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 eighteen (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.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. The FTC also provides information on-line at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

### **For More Information**

The McKnight Group recognizes that you may have questions not addressed in this letter. If you have additional questions, please call 1-800-405-6108 (toll free) during the hours of 8:00am to 8:00pm, Monday through Friday (excluding U.S. national holidays).

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you.

Sincerely,

The McKnight Group

### **Additional Important Information**

**For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina:** It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

---

**For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:**

It is required by state laws to inform you that 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](http://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.

---

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

---

**For residents of Oregon:** State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

---

**For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:** You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**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](http://www.coag.gov).

**For District of Columbia residents,** the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, [www.oag.dc.gov](http://www.oag.dc.gov).

**For New Mexico residents,** state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 at [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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 Rhode Island residents,** this incident involves 0 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov)

---

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

**Rhode Island Office of the Attorney General** Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 [www.riag.ri.gov](http://www.riag.ri.gov)

**North Carolina Office of the Attorney General** Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 [www.ncdoj.com](http://www.ncdoj.com)

**Federal Trade Commission** Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**New York Office of Attorney General** Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>; *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>;

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

---

**For residents of all states:**

**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](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 at the bottom of this page.

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

**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. If you request a security freeze from a consumer reporting agency, there may be a fee up to \$5 to place, lift or remove the security freeze. 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  
[equifax.com/personal/credit-report-services/](http://equifax.com/personal/credit-report-services/)  
1-800-349-9960

**Experian Security Freeze**  
P.O. Box 9554  
Allen, TX 75013  
[experian.com/freeze/center.html](http://experian.com/freeze/center.html)  
1-888-397-3742

**TransUnion Security Freeze**  
P.O. Box 160  
Woodlyn, PA 19094  
[transunion.com/credit-freeze](http://transunion.com/credit-freeze)  
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.