



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

July 3, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Fellowship Village located at 8000 Fellowship Road, Suite 1C, Basking Ridge, NJ 07920, and are writing to notify your office of an incident that may affect the security of certain personal information relating to thirteen (13) Maryland residents. Fellowship reserves the right to supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, Fellowship Village does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around August 9, 2023, Fellowship Village became aware of suspicious activity affecting certain systems within its network. Fellowship Village immediately took steps to investigate and contain this activity. As part of its response to this event, Fellowship Village retained Mullen Coughlin as privacy counsel. Mullen Coughlin engaged a third-party digital forensic investigation firm on Fellowship Village's behalf to assist with containment and remediation of the incident and to conduct a legally privileged investigation to confirm the nature and scope of the unauthorized activity. Through this investigation, Fellowship Village determined that certain of its systems were accessible to an unknown actor between July 27, 2023, and August 9, 2023, and certain files on those systems were viewed or copied without authorization during that time frame. As such, Fellowship Village, with the assistance of third-party data review specialists, conducted a time-intensive and thorough programmatic and manual review of the data which was stored on the impacted systems and determined that certain sensitive information was contained therein.

Following this review, Fellowship Village conducted additional review of its records to confirm the identities and contact information for potentially affected individuals in order to provide notification. This review was recently completed.

The information that could have been subject to unauthorized access includes name, Social Security number, financial account information, medical information, and health insurance information.

Notice to Maryland Residents

Fellowship Village provided preliminary notice to its current residents, with an offer of credit monitoring, on October 6, 2023. On or about July 3, 2024, Fellowship Village provided written notice of this incident to thirteen (13) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Fellowship Village previously provided preliminary website posting and notice to certain jurisdictions statewide media on October 8, 2023.

Other Steps Taken and To Be Taken

Upon discovering the event, Fellowship Village moved quickly to investigate and respond to the incident, assess the security of Fellowship Village systems, and identify potentially affected individuals. Further, Fellowship Village notified federal law enforcement regarding the event. Fellowship Village is also working to implement additional safeguards and training to its employees. Fellowship Village is providing access to credit monitoring services for one (1) year through Transunion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Fellowship Village is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Fellowship Village is providing individuals with 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, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Fellowship Village is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Office of the Attorney General
Attn: Security Breach Notification
July 3, 2024
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

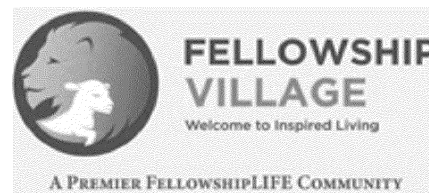
EJF/jlt
Enclosure

EXHIBIT A

Fellowship Village
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Via First-Class Mail

P



July 1, 2024

Re: Notice of Data Breach

Dear [REDACTED]

Fellowship Village is writing to inform you of a recent event that may impact the privacy of some of your information. Although at this time there is no indication that your information has been used to commit identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and steps you may take to help protect your information, should you feel it necessary to do so.

What Happened? On or around August 9, 2023, we became aware of suspicious activity relating to certain systems within our network. We immediately launched an investigation to determine the full nature and scope of the activity and to restore functionality to the impacted systems. The investigation determined there was unauthorized access to Fellowship Village's network between July 27, 2023, and August 9, 2023, and that certain files and folders were or may have been taken without authorization during that time. Upon becoming aware of this information, Fellowship Village began a diligent and comprehensive review process to identify sensitive information that was contained within the impacted files, and to identify the individuals whose information may have been impacted. Fellowship Village then worked to identify appropriate contact information for the impacted individuals. That process was recently completed and we are notifying you because the investigation determined certain information related to you was contained within the impacted files.

What Information Was Involved? The investigation determined the following types of information related to you were present in the impacted systems: your name, and financial account information.

What We Are Doing. The confidentiality, privacy, and security of information within our care are among Fellowship Village's highest priorities. Upon learning of the incident, we promptly commenced an investigation and response that included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and investigating to determine the information that may be impacted. We also reported this event to federal law enforcement and government regulators. As part of our ongoing commitment to the privacy of information in their care, we are reviewing its policies, procedures and processes to reduce the likelihood of a similar future event.

As an added precaution, we are also offering you 12 months of credit monitoring and identity restoration services at no cost to you through Transunion. Enrollment instructions are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Personal Information* for useful information on what you can do to better protect against possible misuse of information. You may also enroll in the complimentary credit monitoring services we have provided for you.

000010102G0500

P

For More Information. If you have questions, you can call our dedicated assistance line at 1-800-405-6108 Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays). You may also write to Fellowship Village at 8000 Fellowship Road, Basking Ridge, NJ 07920.

Sincerely,

Fellowship Village

Steps You Can Take to Help Protect Personal Information

Enroll in Credit Monitoring 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:
7FED316AFDDA

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.



Monitor Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state attorney general. This notice has not been delayed by law enforcement.

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 Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There is approximately 1 Rhode Island resident that may be impacted by this event.