



David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, NY 11201
dmcmillan@constangy.com
Mobile: 718.614.8371

November 12, 2024

VIA EMAIL

Attorney General Anthony Brown
Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy Brooks Smith & Prophete LLP represents Familylinks Inc. ("Familylinks") in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On May 3, 2024, Familylinks discovered suspicious activity with one of its employee's email accounts. Familylinks immediately initiated an investigation of the matter, engaging independent cybersecurity experts to assist with the process. As a result of this investigation, Familylinks determined that certain emails and attachments may have been acquired without authorization on May 3, 2024. Following a comprehensive review of the affected data, which concluded on October 3, 2024, Familylinks learned that certain personal and / or protected health information may have been impacted in connection with this incident.

Familylinks then worked diligently to identify current address information for purposes of promptly providing notification. Importantly, Familylinks has no evidence of the misuse or attempted misuse of any potentially impacted information.

The information that may have been affected by this incident varies by individual, but includes individuals' names, dates of birth, payment card numbers in combination with information allowing access to the accounts, usernames and associated passwords, medical information – such as provider name, treatment information, Medical Record Numbers, prescription information, and health insurance information - and Social Security numbers.

2. Number of Maryland residents notified.

Familylinks notified two (2) Maryland residents of this incident via first class U.S. mail on November 12, 2024. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Familylinks discovered this incident, it took steps to secure its email tenant and launched an investigation to determine whether personal and / or protected health information had been accessed or acquired without authorization. Familylinks has also implemented additional safeguards to help ensure the security of its environment and to reduce the risk of a similar incident occurring in the future.

Familylinks has established a toll-free call center through Equifax, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while Familylinks is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Familylinks is also providing complimentary identity protection services to individuals whose Social Security numbers were affected by the incident.

4. Contact information.

Familylinks remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink, appearing to read "D. McMillan", followed by a horizontal line extending to the right.

David McMillan
Partner, Cybersecurity & Data Privacy Team

Enclosure: Sample Notification Letter



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

To Enroll, Please Visit:

www.equifax.com/activate

Enrollment Code: <<Activation Code>>

<<Date>>

Subject: Notice of Data <<Variable Header>>

Dear <Full Name>:

We are writing to inform you about a data security incident that may have affected your personal or protected health information held in the digital systems of Familylinks Inc. ("Familylinks"), located in Pittsburgh, Pennsylvania. This letter is to notify you of the incident, offer you complimentary identity protection services, and inform you about steps you can take to help protect your personal information.

What Happened: On May 3, 2024, Familylinks discovered suspicious activity with one of its employee's email accounts. Familylinks immediately initiated an investigation of the matter, engaging independent cybersecurity experts to assist with the process. As a result of this investigation, Familylinks determined that certain emails and attachments may have been acquired without authorization on May 3, 2024. Following a comprehensive review of the affected data, which concluded on October 3, 2024, Familylinks learned that your personal and / or protected health information may have been impacted in connection with this incident. Please note that Familylinks has no evidence of the misuse or attempted misuse of any of this information.

What Information Was Involved: The data that could have potentially been accessed by the unauthorized party included your name and <<Data Elements>><<Variable data 1>>.

What We Are Doing: As soon as Familylinks discovered this incident, it took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. Familylinks is also offering you <<12/24>> months of complimentary identity protection services through Equifax. This service helps detect possible misuse of your information and provides you with identity protection support. The deadline to enroll in these services is <<Enrollment Deadline>>.

What You Can Do: You can follow the recommendations included with this letter to help protect your information. In addition, you can also enroll in Equifax's complimentary identity protection services by going to the link noted above.

For More Information: Further information about how to protect your personal information appears on the following pages. If you have any questions regarding the incident or need assistance, please do not hesitate to call 855-277-9409 Monday through Friday between 9:00 a.m. and 9:00 p.m. Eastern.

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

Sincerely,

A handwritten signature in black ink, appearing to read 'M. Ulizio', with a horizontal line extending to the right.

Mallory Ulizio, Privacy Officer
Familylinks Inc.
401 N. Highland Ave.
Pittsburgh, PA 15206

Steps You Can Take to Help Protect Your Personal 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 (the “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 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

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
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 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
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

NC Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers
877-566-7226

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.