



Melissa Sachs, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
msachs@constangy.com
Mobile: 215.983.4404

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

June 28, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Telephone: 410-576-6491
Email: idtheft@oag.state.md.us

Re: Faison Enterprises, Inc. - Notice of Data Security Event

To Attorney General Anthony G. Brown:

We represent Faison Enterprises, Inc. ("Faison") located at 1011 East Morehead St., Suite 150, Charlotte, North Carolina 28204, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately twenty-nine (29) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Faison 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.

1. Nature of the Data Event

On February 29, 2024, Faison experienced a network disruption and initiated an investigation to determine the full nature and scope of the incident. The investigation determined that certain files may have been accessed and/or acquired without authorization. After a thorough review of those files, on or about May 30, 2024, Faison determined that some personal information was identified as being contained within the potentially affected data.

The information that could have been subject to unauthorized access includes first and last name, as well as Social Security number, driver's license or state identification number, financial account number and financial account access information.

2. Notice to Maryland Residents

On or about June 28, 2024, Faison provided written notice of this incident to twenty-nine (29) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

3. Other Steps Taken and To Be Taken

Upon discovering the event, Faison moved quickly to investigate and respond to the incident, assess the security of Faison systems, and identify potentially affected individuals. Further, Faison notified federal law enforcement regarding the event. Faison is also working to implement additional safeguards and training to its employees. Faison is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Faison is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Faison 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.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at 267.219.8332.

Very truly yours,



Melissa Sachs of
Constangy, Brooks, Smith & Prophete LLP

Exhibit A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Subject: <<b2b_text_1 (Notice of Data Breach/Security Incident)>>

Dear <<first_name>> <<last_name>>:

We are writing to inform you of a recent incident that may have affected your personal information. At Faison Enterprises, Inc. ("Faison") we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to help protect your personal information, and offering you complimentary identity monitoring services.

What Happened. On February 29, 2024, Faison experienced a network disruption and initiated an investigation to determine the full nature and scope of the incident. The investigation determined that certain files may have been accessed and/or acquired without authorization. After a thorough review of those files, on or about May 30, 2024, we determined that some of your personal information was identified as being contained within the potentially affected data.

What Information Was Involved. The information may have included your <<b2b_text_2 (name, data elements)>>.

What We Are Doing. As soon Faison discovered the incident we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. We notified the Federal Bureau of Investigation and continue to cooperate as necessary to hold the perpetrators accountable.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<Monitoring Term Length (Months)>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

- Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.
- You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
- Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also activate in the complementary services offered to you by going to info.krollmonitoring.com. Please have your membership number ready.

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 [\[Toll Free Number\]](#), Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding holidays). 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,

Faison Enterprises, Inc.

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, Faison recommends 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

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 <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.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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, which may or may not be listed below, but should be easy to find on your Attorney General's website.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov/
1-888-743-0023

New York Attorney General

The Capitol
Albany, NY 12224-0341
<https://ag.ny.gov/file-complaint>
1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.