



Sean B. Hoar
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, Oregon 97035
SHoar@constangy.com
503.459.7707

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

December 5, 2023

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
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 Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Hi-School Pharmacy in connection with a data security incident described below. This notice is being sent pursuant to Md. Code Ann., Comm. Law § 14-3504.

On November 3, 2023, Hi-School Pharmacy experienced a disruption in its computer network. It immediately initiated an investigation and engaged digital forensic experts to assist with the process. The forensic investigation determined that certain personal information may have been acquired without authorization during the incident. They conducted a thorough review of the affected information and on November 21, 2023, determined that information involving three (3) Maryland residents was involved. They then engaged a consumer remediation firm and worked with them to provide notification and identity protection services as soon as possible. For the two (2) Maryland residents for whom a Social Security number may have been affected, remediation services included an offer of credit monitoring. A sample copy of that notification letter which was sent on December 5, 2023, is attached.

Should you have any questions or need additional information, please contact me at 503.376.5932 or shoar@constangy.com, or Alyssa Pearce at 984.600.4284 or apearce@constangy.com.

Sincerely,

A handwritten signature in blue ink that reads "Sean B. Hoar".

Sean B. Hoar
Partner and Chair, Constangy Cyber Team

Encl. Sample Notification Letter

Hi-School Pharmacy
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



December 5, 2023

Subject: Notice of Data Security Incident

Dear [REDACTED]:

I am writing to inform you of a data security incident that may have affected your personal information. At Hi-School Pharmacy, we take the privacy and security of personal information very seriously. This is why we are informing you of the incident and providing you with steps you can take to protect your personal information.

What Happened? On November 3, 2023, Hi-School Pharmacy experienced a disruption in our computer network. We immediately initiated an investigation and engaged digital forensic experts to assist us with the process. The forensic investigation determined that certain personal information may have been acquired without authorization during the incident. We conducted a thorough review of the affected information and on November 21, 2023 determined that your information was involved. We then engaged a consumer remediation firm and worked with them to provide you notification and identity protection services as soon as possible.

What Information Was Involved? The information may have included your [REDACTED]

What We Are Doing. As soon as we discovered this incident, we took the steps described above. We also notified the FBI and will provide whatever cooperation may be necessary to hold the perpetrators accountable. We have also implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. We are also offering you complimentary credit monitoring and identity protection services through CyberScout, a leader in consumer identity protection. These services include twelve (12) months of credit monitoring, report and score services through TransUnion, identity protection and resolution services, and a \$1 million identity fraud loss reimbursement policy.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information.

How do I enroll for the free services? To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/hsp> 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.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-833-519-0755 Monday through Friday from 5 am to 5 pm Pacific 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,

A handwritten signature in black ink, appearing to read "Jack Holt", with a stylized flourish extending to the right.

Jack Holt, President

STEPS YOU CAN TAKE TO 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 (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 2000
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.

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, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

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

Oregon Attorney General

1162 Court Street NE
Salem, OR 97301
doj.state.or.us
1-877-877-9392

Washington Attorney General

800 5th Avenue, Suite 2000
Seattle, WA 98104-3188
atg.wa.gov
1-206-464-6684/1-800-551-4636

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.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf.

Hi-School Pharmacy
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



December 5, 2023

Subject: Notice of Data Security Incident

Dear [REDACTED]:

I am writing to inform you of a data security incident that may have affected your personal information. At Hi-School Pharmacy, we take the privacy and security of personal information very seriously. This is why we are informing you of the incident and providing you with steps you can take to protect your personal information.

What Happened? On November 3, 2023, Hi-School Pharmacy experienced a disruption in our computer network. We immediately initiated an investigation and engaged digital forensic experts to assist us with the process. The forensic investigation determined that certain personal information may have been acquired without authorization during the incident. We conducted a thorough review of the affected information and on November 21, 2023 determined that your information was involved. We then engaged a consumer remediation firm and worked with them to provide you notification and identity protection services as soon as possible.

What Information Was Involved? The information may have included your [REDACTED].

What We Are Doing. As soon as we discovered this incident, we took the steps described above. We also notified the FBI and will provide whatever cooperation may be necessary to hold the perpetrators accountable. We have also implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-833-519-0755 Monday through Friday from 5 am to 5 pm Pacific 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,

A handwritten signature in black ink, appearing to read "Jack Holt".

Jack Holt, President

STEPS YOU CAN TAKE TO 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 (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 2000
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.

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, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

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

Oregon Attorney General

1162 Court Street NE
Salem, OR 97301
doj.state.or.us
1-877-877-9392

Washington Attorney General

800 5th Avenue, Suite 2000
Seattle, WA 98104-3188
atg.wa.gov
1-206-464-6684/1-800-551-4636

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 http://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf.