



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

February 28, 2023

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 Incident

To Whom It May Concern:

We represent Hatch Bank, located at 1001 West San Marcos Blvd. #125, San Marcos, CA 92078, and are writing to notify your office of an incident that may affect the security of certain personal information relating to three thousand four hundred thirty-seven (3,437) Maryland residents. The investigation into this matter is ongoing, and this may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Hatch Bank does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data incident notification statute, or personal jurisdiction.

Nature of the Data Incident

On January 29, 2023, Fortra experienced a cyber incident when they learned of a vulnerability located in their software. On February 3, 2023, Hatch Bank was notified by Fortra of the incident and learned that its files contained on Fortra's GoAnywhere site were subject to unauthorized access. Fortra's investigation determined that there was unauthorized access to the site account from January 30, 2023, to January 31, 2023. Hatch Bank immediately took steps to secure its files and then launched a diligent and comprehensive review of relevant files to determine the information that may have been impacted. Hatch Bank then worked to identify contact information for the impacted individuals. That process completed on February 7, 2023.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maryland Residents

On or about February 28, 2023, Hatch Bank provided written notice of this incident to three thousand four hundred thirty-seven (3,437) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit A**. Hatch Bank's investigation into this incident is ongoing and this notification may be supplemented if it is determined that a significant number of additional Maryland residents were impacted by this incident.

Other Steps Taken and To Be Taken

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

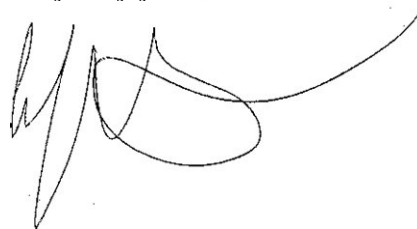
Additionally, Hatch Bank is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Hatch Bank is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer 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.

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

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact us at (267) 930-1509.

Very truly yours,

A handwritten signature in black ink, appearing to read 'GJB', with a long, sweeping horizontal line extending to the right.

Gregory J. Bautista of
MULLEN COUGHLIN LLC

EXHIBIT A

Hatch Bank
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



February 28, 2023

NOTICE OF [SECURITY INCIDENT/DATA BREACH]

Dear [REDACTED]:

Hatch Bank writes to inform you of a recent incident that may impact the privacy of some of your information. On February 3, 2023, Hatch Bank received notice that our third-party technology vendor, Fortra, suffered a cyber incident. While we are currently unaware of any actual or attempted misuse of your information, we are providing you with information about the incident, our response, and steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened? On January 29, 2023, Fortra experienced a cyber incident when they learned of a vulnerability located in their software. On February 3, 2023, Hatch Bank was notified by Fortra of the incident and learned that its files contained on Fortra's GoAnywhere site were subject to unauthorized access. Fortra's investigation determined that, between January 30 and January 31, 2023, someone without authorization had access to certain files stored within Fortra's GoAnywhere site. We then launched a diligent and comprehensive review of relevant files to determine the information that may have been impacted.

What Information Was Involved? On February 7, 2023, we determined the information that may have been impacted by this incident includes your name [REDACTED]. Again, at this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. The confidentiality, privacy, and security of information within our care are among our highest priorities. Upon being notified of this incident, Hatch Bank immediately launched an internal investigation to determine who may have been affected by this third-party incident.

As an added precaution, we are providing you with access to [12/24] months of credit monitoring and identity protection services through Cyberscout at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Your Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, which contains information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against potential incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You will also find information on how to enroll in the credit monitoring services offered. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. We understand that you may have questions that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 1-833-570-2931, which is available Monday through

000010102G0500

P

Friday, between the hours of 8:00 a.m. and 8:00 p.m. Eastern Time, excluding major U.S. holidays. You may also write to Hatch Bank at 1001 West San Marcos Blvd. #125, San Marcos, CA 92078.

How We Received Your Information. Your information was received by Hatch Bank in connection with a loan you applied for through [REDACTED]. Hatch Bank either reviewed your application to issue a credit decision or is the owner of your current loan or credit card account issued through your relationship with [REDACTED]. It is important to note that Fortra is still investigating their incident and that [REDACTED] system was not directly involved in Fortra's incident associated with this notice from Hatch Bank.

Sincerely,

Hatch Bank

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring** services at no charge. These services provide you with alerts for 24 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.



To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/hatchbank> 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.

Monitor Your 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 credit 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, 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 credit freeze, please contact the three major credit reporting bureaus listed below:

00001020280000

P

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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, DC 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; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Hatch Bank is located at 1001 West San Marcos Blvd., San Marcos, CA 92078.

For New Mexico residents, you 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 bureaus 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 violator. 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 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, you have the right to obtain any police report filed in regard to this incident. There are 160 Rhode Island residents impacted by this incident.