



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

RECEIVED

MAY 10 2021

CONSUMER PROTECTION

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

1127 High Ridge Road, #301  
Stamford, CT 06905

May 5, 2021

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent STCR Business Systems, Inc. (“STCR”) located at 10 Prospect Street, Endwell, New York 13760, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. By providing this notice, STCR does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On February 24, 2021 STCR identified suspicious activity related to certain employee email accounts. We immediately worked to secure the e-mail environment and launched an investigation into the nature and scope of the incident. The investigation confirmed STCR systems were not impacted, and the activity was limited to the cloud hosted Microsoft Outlook 365 email environment, which is separate from the STCR environment. With the assistance of third-party computer forensic specialists, we investigated this incident to confirm whether any sensitive information was viewed or removed from STCR’s systems without authorization. On April 12, 2021, STCR determined that the information that could have been subject to unauthorized access includes name and Social Security Number.

### **Notice to New Hampshire Resident**

On or about May 5, 2021, STCR provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, STCR moved quickly to investigate and respond to the incident, assess the security of STCR systems, and notify potentially affected individuals. STCR is also working to implement additional safeguards and training to its employees. STCR is providing access to credit monitoring services for one (1) year, through Experian IdentityWorks, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, STCR 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. STCR is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

### **Contact Information**

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

Very truly yours,



Gregory J. Bautista of  
MULLEN COUGHLIN LLC

GJB /ams

# Exhibit A



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

May 5, 2021

G4360-L01-0000001 T00001 P001 \*\*\*\*\*AUTO\*\*MIXED AADC 159



SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, ST 12345-6789



### NOTICE OF SECURITY INCIDENT

Dear Sample A. Sample:

STCR Business Systems (“STCR”) is writing to make you aware of an incident that may affect the security of some of your personal information. Safeguarding our employees’ information is very important to us, and this letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

**What Happened?** On February 24, 2021 STCR identified suspicious activity related to certain employee email accounts. We immediately worked to secure the e-mail environment and launched an investigation into the nature and scope of the incident. The investigation confirmed STCR systems were not impacted, and the activity was limited to the cloud hosted Microsoft Outlook 365 email environment, which is separate from the STCR environment. With the assistance of third-party computer forensic specialists, we investigated this incident to confirm whether any sensitive information was viewed or removed from STCR’s systems without authorization.

**What Information Was Involved?** Our investigation to date determined the following types of your personal information **potentially** affected by this incident are your name, and social security number.

**What We Are Doing.** Information security is among STCR’S highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems. We are reviewing existing security policies and implemented additional cybersecurity measures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. We are also reporting to regulatory officials, as required.

As an added precaution, we are offering you access to credit monitoring and identity theft protection services for 12 months at no cost to you, through Experian Identity Works. You may find information on how to enroll in these services in the enclosed “Steps You Can Take to Protect Your Information.” We encourage you to enroll in these services as we are not able to do so on your behalf.

0000001



G4360-L01

**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 free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Protect Your Information.*"

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (833) 704-9394, between the hours of Monday through Friday from 6 a.m. to 8 p.m. PST and Saturday/Sunday from 8 a.m. to 5 p.m. PST. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,



Farrell McKenna  
Director of Operations

## STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

### Enroll in EXPERIAN IDENTITYWORKS MEMBERSHIP

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: July 31, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 704-9394 by July 31, 2021. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 704-9394. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

\* Offline members will be eligible to call for additional reports quarterly after enrolling

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

### 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](http://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.

0000001



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 1-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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	833-395-6938
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](http://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 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/>.

STATE OF NH  
DEPT OF JUSTICE

2021 MAY 10 PM 1:24