HINSHAW & CULBERTSON LLP
Attorneys at Law
800 Third Avenue
13th Floor
New York, NY 10022

212-935-1166 (fax)
www.hinshawlaw.com

Cathy Mulrow-Peattie

October 23, 2024

VIA E-MAIL
Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

RE: Notice of Data Security Incident

We represent RRCA Accounts Management Inc. ("RRCA") located at 201 E 3rd St Sterling, IL. We are writing to inform you that we had a data security incident that may impact 7 New Hampshire residents personal information.

Notice to New Hampshire Residents

The anticipated date of notice to be provided to consumers as required by the Health Insurance Portability and Accountability Act of 1996 ("HIPPA") and applicable data breach state requirements is on or around October 18, 2024. A copy of the form notification letter is attached hereto, as Exhibit A.

What Steps Have We Taken

Additionally, RRCA has provided the affected 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. RRCA 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.

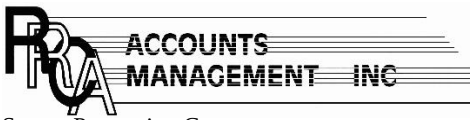
This letter does not waive any rights on behalf of RRCA and is being provided for notification purposes only.

Should you have further questions or concern, please contact the undersigned at .

Sincerely,
HINSHAW & CULBERTSON LLP

Cathy Mulrow-Peattie

Exhibit “A”



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>,

We are contacting you to notify you that we are a vendor of one or several of your health care providers or other business companies which you may owe a payment, and we experienced a security incident that may have involved your personal information.

WHAT HAPPENED?

We experienced a security incident from a ransomware attack from the Play threat actors on June 6, 2024, but only learned about the release of your personal information from this security incident on August 20, 2024, as the criminals covered their tracks. We quickly took action to stop the activity. Cybercriminals illegally accessed our computer systems without permission.

WHAT INFORMATION WAS INVOLVED?

We also informed our clients, your health care providers or other business companies for which we collect outstanding payments, about this event and what personal information may have been accessed. The personal information that may have been accessed by a third party includes your contact information (such as

WHAT ARE WE DOING?

We have been diligently working with law enforcement and forensic investigators to conduct a thorough review of the potentially affected data. We have implemented additional organizational, technical and administrative security measures to prevent the reoccurrence of such a breach and to protect the privacy of our customers.

WHAT CAN YOU DO?

We are notifying you so that you can take action which will assist to minimize or eliminate potential harm. We strongly advise you to take preventive measures to help prevent and detect any misuse of your information.

To help protect you, we have retained CyEx, a specialist in identity theft prevention to provide you with <<12/24>> months of credit monitoring services and identity theft services, free of charge. You can enroll in the program by following the attached directions.

As a first step, we recommend that you closely monitor your financial and health accounts and if you see any unauthorized activity, you should promptly contact your financial institution or health insurance carrier.

To further protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other two on your behalf. You will then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each.

- Equifax (888)766-0008 or www.fraudalert.equifax.com
- Experian (888) 397-3742 or www.experian.com
- TransUnion (800) 680-7289 or www.transunion.com

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot a problem and address it quickly.

We sincerely apologize for the inconvenience this incident has caused you. Please be advised that we will keep you informed of any developments in the investigation which may be of importance to you.

Who to call or contact with questions?

If you have further questions or concern, please contact the undersigned at this special telephone number 1-855-277-4799, Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time, except holidays.

Sincerely,

RRCA Accounts Management Team

Identity Defense

Enter your Activation Code: **<<Activation Code>>**
Enrollment Deadline: **<<Enrollment Deadline>>**
Service Term: <<12/24>> months*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance

Enrollment Instructions

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/rrca

1. **Enter your unique Activation Code** <<Activation Code>>
   Enter your Activation Code and click 'Redeem Code'.
2. **Create Your Account**
   Enter your email address, create your password, and click 'Create Account'.
3. **Register**
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. **Complete Activation**
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.