SpencerFane

*Shawn E. Tuma*
*Direct Dial: 972.324.0317*
*stuma@spencerfane.com*

October 8, 2020

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

**Re: Notification of Data Security Incident**

Dear Attorney General Gordon MacDonald:

Be advised that the undersigned and this law firm have been retained to represent Niibin, LLC, d/b/a Cash Aisle in connection with the recent data security incident described below.

On September 15, 2020, Cash Aisle learned from its third party service provider, Preferred Call Services ("PCS"), that email accounts of PCS which contained the personal information of Cash Aisle's customers were compromised. Cash Aisle utilizes the services of PCS to provide call center services on its behalf. PCS notified Cash Aisle that it initially discovered anomalous activity on its computer systems on or around July 2, 2020. This incident involved an unauthorized individual gaining access to email accounts maintained by PCS and downloading some of the contents of the email accounts. While Cash Aisle does not have evidence that any information was used for fraudulent purposes, it is unable to conclusively rule out the possibility that personal information was compromised as a result of this incident. Therefore, out of an abundance of caution, Cash Aisle will notify all customers who may have been impacted by this incident.

The compromised email accounts may have contained information such as names, addresses, dates of birth, Social Security numbers, driver's license numbers, bank account numbers, routing numbers, or payment card information.

Cash Aisle is offering affected individuals MyIDCare™ identity theft protection services through ID Experts®, the data breach and recovery services expert. MyIDCare™ services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

Because this incident involves the computer system of Cash Aisle's service provider, Cash Aisle is limited in its ability to ensure this type of incident does not reoccur. Cash Aisle has remained in constant communication with PCS to ensure its continued commitment to protect the information entrusted in its care. Upon learning of this incident, PCS changed the passwords of its email accounts, performed scans on all of its computer systems, updated its domain and user level settings, and performed additional computer security changes.

SpencerFane

PCS engaged a third party cybersecurity firm to manually analyze the impacted information and has taken additional measures and corrective actions to remediate and mitigate the effects of this incident and help prevent a similar incident from occurring in the future.

Cash Aisle mailed notification letters to 2 residents of New Hampshire on October 5, 2020. A sample copy of the notification letter is enclosed.

Respectfully,
**Spencer Fane, LLP**

By: _____
Shawn E. Tuma, Partner

Enclosure: Notice of Data Breach

C/O ID Experts
[Return address]
[City], [State] [Zip]

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect

Enrollment Code: <<XXXXXXXX>>

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

October 5, 2020

**Notice of Data Breach**

Dear <<Name 1>>,

**What Happened**

We are writing to inform you of an incident that involved your personal information. On September 15, 2020, we learned that the email account of our third-party service provider, Preferred Call Services ("PCS"), which contained your personal information was compromised. Cash Aisle utilizes the services of PCS to provide call center services on our behalf. This incident involved an unauthorized individual gaining access to email accounts maintained by PCS and downloading some of the contents of the email account. While we do not have evidence that any of your information was used for fraudulent purposes we are unable to conclusively rule out the possibility that your personal information was compromised as a result of this incident. Therefore, out of an abundance of caution, Cash Aisle is notifying you of this incident.

We deeply regret that this has occurred and apologize for any inconvenience or concern caused by this incident.

**What Information Was Involved**

The compromised email accounts may have contained information such as your name, address, date of birth, Social Security number, driver's license number, bank account number, routing number, or payment card information.

**What We Are Doing**

We have remained in constant communication with PCS to ensure its continued commitment to protect the information entrusted in its care. Upon learning of this incident, PCS changed the passwords of its email accounts, performed scans on all of its computer systems, updated its domain and user level settings, and performed additional computer security changes.

PCS engaged a third party cybersecurity firm to manually analyze the impacted information and has taken additional measures and corrective actions to remediate and mitigate the effects of this incident and help prevent a similar incident from occurring in the future.

Cash Aisle is also working to minimize the impact of this incident and identify additional actions we can take to reduce the risk of it recurring and will make necessary adjustments to help ensure the security of your data going forward.

**What You Can Do**

The events that have occurred do not automatically mean that you are a victim of identity theft. However, we encourage you to remain vigilant, to continually review your credit report, bank account activity, and bank statements for irregularities or unauthorized items, and to immediately report any unauthorized charges to your financial institution.

We recommend you take one or more of the actions listed in the enclosed Recommended Steps document.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare™ services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare™ will help you resolve issues if your identity is compromised as a result of this data incident.

**For More Information**

Please contact ID Experts with any questions you may have concerning this incident and to enroll in free MyIDCare™ services by calling 1-800-939-4170 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare™ experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is January 5, 2021.

We value your privacy and sincerely regret any inconvenience this matter may cause. Our relationship with you, your confidence in our ability to safeguard your personal information, and your peace of mind are very important to us.

Kindest Regards,

_____

Jessi Lorenzo, President
Niibin, LLC dba Cash Aisle

**Niibin, LLC dba Cash Aisle**
**Po Box 872**
**Lac du Flambeau, WI 54538**

**LDF Holdings, LLC**
**Po Box 231**
**Lac du Flambeau, WI 54538**

**Recommended Steps to help Protect your Information**

**1. Telephone.** Contact the ID Experts call center at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**2. Review your credit reports**. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**3. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

**Credit Bureaus**

| Equifax Fraud Reporting | Experian Fraud Reporting | TransUnion Fraud Reporting |
|---|---|---|
| 1-866-349-5191 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 105069 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348-5069 | Allen, TX 75013 | Chester, PA 19022-2000 |
| www.alerts.equifax.com | www.experian.com | www.transunion.com |

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**4. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**5. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them, at https://www.identitytheft.gov/.

**California Residents:** Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

**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 agencies 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 a 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. You can 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.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261