Southeastern Grocers

BI-LO FRESCO y Más HARVEYS supermarket Winn-Dixie

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

NOTICE OF SECURITY BREACH
November 11, 2020

Southeastern Grocers, Inc., a Delaware corporation doing business as Winn-Dixie (the "Company"), hereby provides this Notice of Security Breach to the New Hampshire Attorney General in accordance with Title XXXI Section 359-C:20 of the New Hampshire Statutes.

On September 22 and September 23, 2020, criminal actors committed two brute-force password attacks on the Company's website, www.winndixie.com, using a method called credential stuffing. With this type of attack, the bad actors extract login information for a large number of users from systems they are able to access, and they then use those usernames and passwords to try and access other systems with the hope that people are using the same usernames and passwords for multiple accounts. The Company became aware of the criminal intrusion on the same day of each attack and acted immediately to contain the attacks by addressing system security to stop the malicious activity. After containing the attacks the Company began its investigation and all relevant system logs were gathered and stored for analysis. Shortly after implementing containment measures and updating security measures that could stop the malicious activity, the Company engaged its forensic incident response partner to further analyze, review, and verify the details of the incident. During the course of the Company's investigation, the Company learned that the criminal actors were able to obtain account login information and related personal information for some of the Company's customer loyalty accounts.

Those whose loyalty accounts were impacted in the first attack were sent an email from the Company on September 25, 2020, and those whose loyalty accounts were impacted in the second attack were sent an email from the Company on October 5, 2020. A copy of the text of those emails is attached hereto as Exhibit A. Those emails informed customers of the incident, instructed them that their passwords had been reset to random passwords, and notified them of how to reset their passwords.

According to the Company's records, there are four (4) New Hampshire residents whose loyalty accounts were impacted. The Company intends to mail to these four (4) New Hampshire residents a letter notice in the form attached hereto as Exhibit B on or before November 13, 2020. The Company believes that letter notice includes the content required by Section 359-C:20(IV).

The Company does not collect or store social security numbers or financial information for its customers who have loyalty accounts. For those Company customers whose loyalty accounts were accessed as a result of this attack, only the personal information that customer has provided in connection with the loyalty account could have been compromised, and at most that information would include the customer's name, phone number, email address, date of birth, reward number and PIN, recent points transactions, and loyalty account points balance. This attack was limited to the winndixie.com website; however, the rewards accounts can be used at all Winn-Dixie, BI-LO, Fresco y Más and Harveys store locations. The Company is continuing to thoroughly review the potentially affected systems and files and is also working closely with forensic investigators, legal counsel and law enforcement to ensure the incident is properly addressed.

The Company and its Information Security Team have already adopted additional security measures to help prevent a recurrence of such an attack, and the Company will be investigating further security measures as it concludes the investigation. Any new security measures will be designed to protect the privacy of the Company's customers.

For additional information regarding the breach, please contact:

Name:	M. Sandlin Grimm
Title:	Chief Legal Officer/Secretary
Company:	Southeastern Grocers, Inc.
Address:	8928 Prominence Parkway, #200 Jacksonville, FL 32256
Telephone Number:	904.783.5473
Email Address:	sandygrimm@segrocers.com

Exhibit A

Initial Email Instructions

(see attached)

WD Banner Customer Account Breach

Subject Line: Notification of Account Issue

Dear [customer],

At Winn-Dixie, we pride ourselves on a safe and rewarding shopping experience that our customers can always count on.

This week, winndixie.com was maliciously targeted and attacked, affecting some of our Winn-Dixie rewards accounts. The situation was quickly contained and is under control.

Although this only represented a fraction of 1% of our total accounts, we take the security of every customer account with equal importance. We wanted to inform you as soon as possible of this issue, as this is a top priority for our organization.

What We Know

- Your Winn-Dixie rewards account information was likely accessed as a result of this attack.
- This information would be limited to the personal information, such as your name and phone number, associated with your account. As a reminder, we DO NOT store any personal financial information or Social Security numbers within the system.
- This attack was limited to winndixie.com; however, rewards accounts can be used at all Winn-Dixie, BI-LO, Fresco y Más and Harveys Supermarket locations.

Actions Taken

- We have assigned a new, randomized password to your account so that any additional malicious activity would be prohibited.
- Our Information Security team has created new protections in our system to better identify and prevent these attacks from occurring in the future.
- We have carefully analyzed our customer accounts so that we can accurately, and quickly, restore any potential lost value of rewards points in your account.

Next Steps

- Please [click here] to reset your account password. Please DO NOT USE the password originally used with this rewards account.
- If you have any questions or concerns, please contact Customer Care at (844) 745-0463 and we will do all we can to assist you.

We apologize for this inconvenience and value your business. Thank you for being a loyal shopper with Winn-Dixie.

Southeastern Grocers, Inc.
8928 Prominence Parkway, #200, Jacksonville, FL 32256
Local: 904.783.5000 Toll Free: 1.800.967.9105
www.SEGrocers.com

Exhibit B

New Hampshire Customer Notice

(see attached)

Southeastern Grocers, Inc.
8928 Prominence Parkway, #200, Jacksonville, FL 32256
Local: 904.783.5000 Toll Free: 1.800.967.9105
www.SEGrocers.com

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[DATE]

NOTICE OF DATA BREACH

At Winn-Dixie, we pride ourselves on a safe and rewarding shopping experience that our customers can always count on.

On September 22nd, and again on September 23, our website, www.winndixie.com, was maliciously targeted and attacked. The attack affected some of our Winn-Dixie rewards accounts, which can be used across our family of stores, including, BI-LO, Fresco y Más, Harveys and Winn-Dixie stores. The situation was quickly contained and is under control.

Although less than 1% of our total loyalty accounts were impacted by this attack, we believe the security of every customer account is equally important. Because of that importance, we wanted to inform you of this issue as soon as possible.

WHAT HAPPENED?

On September 22 and September 23, 2020, criminal actors committed two brute-force password attacks on our website, www.winndixie.com, using a method called credential stuffing. With this type of attack, the bad actors extract user login information from other systems they are able to access, and they then use those usernames and passwords to try and access other systems with the hope that people are using the same usernames and passwords for multiple accounts. We became aware of the criminal intrusion on the same day of each attack and acted immediately to contain the attacks by addressing system security to stop the malicious activity. After containing the attacks we began our investigation and all relevant system logs were gathered and stored for analysis. Shortly after implementing containment measures and updating security measures that could stop the malicious activity, we engaged our forensic incident response partner to further analyze, review, and verify the details of the incident. During the course of our investigation, we learned that the criminal actors were able to obtain account login information and related personal information for some of our customer loyalty accounts, in each of the two attacks.

Customers whose loyalty accounts were impacted in the first attack should have received an email from us on September 25, 2020, and customers whose loyalty accounts were impacted in the second attack should have received an email from us on October 5, 2020. Those emails informed you of the incident, instructed you that your password had been reset to a random password, and notified you of how to reset your password.

WHAT INFORMATION WAS INVOLVED?

We **do not** collect or store Social Security numbers or financial information in conjunction with our loyalty accounts. If you are receiving this letter, your loyalty account was likely accessed as a result of

this attack. Only the personal information that you have provided us in connection with the loyalty account could have been accessed, and at most that information would include your name, phone number, email address, date of birth, reward number, PIN, recent points transactions, and loyalty account points balance. This attack was limited to the winndixie.com website; however, the rewards accounts can be used at all Winn-Dixie, BI-LO, Fresco y Más and Harveys store locations.

WHAT WE ARE DOING

Winn-Dixie values your privacy and deeply regrets that this incident occurred. We are continuing to thoroughly review the potentially affected systems and files, and we will notify you if there are any significant developments that impact your information.

Winn-Dixie and its Information Security Team have already adopted additional security measures to help prevent a recurrence of such an attack, and we will be investigating further security measures as we conclude the investigation. Any new security measures will be designed to protect the privacy of Winn-Dixie's valued customers. Unless you have already changed it as a result of the initial informational emails, your account has a new, randomized password to prevent any additional malicious activity from this attack. We have also carefully analyzed our customer accounts so that we can accurately, and quickly, restore any potential lost value of rewards points in your account.

Winn-Dixie also is working closely with forensic investigators, legal counsel and law enforcement to ensure the incident is properly addressed.

WHAT YOU CAN DO

If you have not already done so, you should promptly reset your password and PIN for your rewards account. If you use the same password or PIN for other accounts, you should reset your credentials on those accounts as well. You can reset your credentials for your loyalty account by calling Customer Care at (844) 745-0463. When resetting credentials for your accounts, your Winn-Dixie loyalty account and any other accounts that used the same credentials, please DO NOT REUSE YOUR OLD PASSWORD OR PIN.

Please also review the attachment to this letter, "Steps You Can Take to Further Protect Your Information." Among other things, this attachment provides the 800 numbers and addresses for the three major credit reporting agencies.

FOR MORE INFORMATION

For further information and assistance, please contact Customer Care at (844) 745-0463 Monday – Friday between 8:00 a.m. and 7:00 p.m. EST or Saturday 8:00 a.m. to 4:00 p.m. EST, or visit www.winndixie.com/about/contact.

We apologize for this inconvenience and value your business. Thank you for being a loyal shopper with Winn-Dixie.

Sincerely,

EXAMPLE

Mahender Bongu
VP, Enterprise Data Services

Steps You Can Take to Further Protect Your Information

- **Review Your Account Statements / Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant, particularly for identity theft and fraud, by reviewing your account statements and monitoring free 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, including your local law enforcement, state attorney general, and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov, call 1-877-ID-THEFT (877-438-4338), or mail your complaint to the FTC at its address 600 Pennsylvania Avenue, NW, Washington, DC 20580, using OMB CONTROL#: 3084-0169. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months. You may also access those reports by visiting http://www.annualcreditreport.com, calling toll-free 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 can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

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 90 days. 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. You can also obtain information from the FTC and consumer reporting agencies about fraud alerts.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov, call 1-877-ID-THEFT (877-438-4338), or contact the FTC at its address 600 Pennsylvania Avenue, NW, Washington, DC 20580, using OMB CONTROL#: 3084-0169. A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, writing to 200 St. Paul Place, Baltimore, MD 21202, or by sending an email to idtheft@oag.state.md.us, or calling 888-743-0023.

New York residents may wish to review information about the incident response and identity theft prevention and protection provided by the New York Attorney General at https://ag.ny.gov/consumer-frauds-bureau/identity-theft or calling 1-800-771-7755.

North Carolina residents may wish to review information provided by the North Carolina Attorney General about preventing identity theft at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.

OTHER IMPORTANT INFORMATION

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze. You may obtain more information about security freezes from the FTC and consumer reporting agencies.