

Lisa Pierce Reisz
Direct Dial (614) 464-8353
Direct Fax (614) 719-4919
Email lpreiz@vorys.com

August 29, 2014

VIA E-MAIL AND U.S. MAIL

James T. Boffetti
Senior Assistant Attorney General
New Hampshire Department of Justice
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301-6397

Re: Shaw's Security Incident

Dear Mr. Boffetti:

We are in receipt of your letter requesting additional information regarding the complaints your office received and the actions undertaken by Shaw's in response to the recent security incident at some of its stores. The Shaw's stores in New Hampshire are operated by New Albertson's, Inc., whose parent corporation is AB Acquisition, LLC headquartered in Boise, Idaho (collectively referred to as "Shaw's"). At this time it is believed that all the Shaw's stores in New Hampshire (a total of twenty-eight) were potentially affected.

Shaw's learned of an unauthorized access to electronic payment card information in some of its stores. While the investigation into this matter is ongoing, Shaw's believes that the affected data could include name, account numbers, expiration date or other numerical information. The appropriate federal law enforcement authorities have been notified, and Shaw's is working closely with its third party IT service provider, Supervalu, to investigate the nature and scope of this incident. Third-party data forensic experts are actively supporting this ongoing investigation. At this point, it has not been determined that any payment card data was in fact stolen.

Although there is still no indication that payment data was acquired, notice of the incident was provided on August 14, 2014. Because Shaw's stores do not collect or keep any of their customers' contact information during payment card transactions, it was not possible to send out customer-specific notice about the incident. Thus, substitute notice in compliance with New Hampshire RSW 359-C:20(III)(d) was provided by: (i) prominently posting notice on the

Senior Assistant Attorney General Boffetti
August 29, 2014
Page 2

Shaw's websites, and (ii) notifying major nationwide and statewide media through the attached press release.

Once the press release was issued, news of the incident was reported by several New Hampshire and Boston, Massachusetts media companies, including WMUR on August 15, 2014, and UnionLeader.com on August 16, 2014. In addition, the Shaw's website homepage contains a "Data Security Update" banner which contains a link to FAQs regarding the incident. Shaw's has and will continue to update these FAQs as more information is available.

Customers whose payment cards may have been affected are eligible for complimentary consumer identity protection services through AllClear ID. The basic AllClear service does not require customer pre-registration and provides customers with identity repair services if a problem arises. For additional protections, customers may enroll in AllClear PLUS, at no charge, which includes identity theft monitoring and a \$1 million identity theft insurance policy for 12 months.

With respect to the complaints your office received, the following attached pages contain summaries of the steps Shaw's has taken to address each complaint.

Shaw's takes its responsibility to its customers very seriously, and will continue to address any concerns that its customers have as a result of this unfortunate incident.

Please contact me with any questions or concerns.

Very truly yours,



Lisa Pierce Reisz

LPR/ESW
Enclosures

FOR IMMEDIATE RELEASE

Media Contact: Christine Wilcox
christine.wilcox@albertsons.com | 208-395-4163

AB Acquisition LLC Confirms Incident Involving Payment Card Data Processing

BOISE, ID – August 14, 2014 – AB Acquisition LLC, which operates Albertsons stores under Albertson’s LLC and ACME Markets, Jewel-Osco, and Shaw’s and Star Markets under New Albertson’s, Inc., recently learned of an unlawful intrusion to obtain credit and debit card payment information in some of its stores. The appropriate federal law enforcement authorities have been notified, and AB Acquisition is working closely with its third party IT services provider, SUPERVALU, to better understand the nature and scope of the incident. Third-party data forensics experts are supporting an ongoing investigation. AB Acquisition has not determined that any cardholder data was in fact stolen, and currently it has no evidence of any misuse of any such data.

AB Acquisition believes that the intrusion has been contained and is confident that its customers can safely use their credit and debit cards in its stores.

Based on the latest information from the ongoing investigation, it appears that the period of unauthorized access may have started on June 22, 2014 (at the earliest) and ended on July 17, 2014 (at the latest).

Based on information we have at this time, Albertsons stores in Arizona, Arkansas, Colorado, Florida, Louisiana, New Mexico, Texas and our two Super Saver Foods Stores in Northern Utah were not impacted by this incident. However, Albertsons stores in Southern California, Idaho, Montana, North Dakota, Nevada, Oregon, Washington, Wyoming and Southern Utah were impacted. In addition, ACME Markets in Pennsylvania, Maryland, Delaware and New Jersey; Jewel-Osco stores in Iowa, Illinois and Indiana; and Shaw’s and Star Markets stores in Maine, Massachusetts, Vermont, New Hampshire and Rhode Island were all impacted by this incident.

“We know our customers are concerned about the security of their payment card data, and we work hard to protect it,” said Mark Bates, Senior Vice President and Chief Information Officer at AB Acquisition LLC. “As soon as we were notified of the incident, we began working closely with SUPERVALU to determine what happened. It’s important to note that there is no evidence at this point that consumer data has been misused.”

Continued Bates, “We understand the inconvenience and concern an incident like this can cause, and we deeply regret that our customers’ data was targeted. ”

Given the continuing nature of the investigation, it is possible that time frames, locations and/or at risk data in addition to that described above will be identified in the future.

More information will be available on the websites at albertsons.com, acmemarkets.com, jewelosco.com, and shaws.com within 24 hours. Although it has not yet been determined whether any

cardholder data was in fact stolen, and there is no evidence to date of any misuse of such data, AB Acquisition LLC is offering customers whose payment cards may have been affected 12 months of complimentary consumer identity protection services through AllClear ID. Customers may visit the websites listed above for further information about the incident and about complimentary consumer identity protection services being offered, or call AllClear ID at 1-855-865-4449 beginning at 2:00pm MT (4:00pm ET) on August 15, 2014.

A free copy of your credit report can also be obtained from each of the credit bureaus once a year by going to <http://www.annualcreditreport.com> or calling 877-322-8228. Hearing impaired consumers can access TDD services at 877-730-4104. We encourage you to monitor these reports, as well as your credit and debit card statements. You may also place a fraud alert or security freeze on your credit report by contacting the credit bureaus as listed below.

About AB Acquisition LLC

Established in 2006, AB Acquisition LLC (“Albertsons”), which operates ACME, Albertsons, Jewel-Osco, Lucky, Shaws, Star Market and Super Saver, and stores under the United Family of stores, Amigos, Market Street and United Supermarkets, is working to become the favorite food and drug retailer in every market it serves. The company is privately owned by Cerberus Capital Management, Kimco Realty Corporation, Klaff Realty, Lubert-Adler Partners, and Schottenstein Stores Corporation, and operates 1,060 stores and 14 distribution centers in 29 states and employs approximately 115,000 associates. For more information, please visit www.Albertsons.com.

###

You may also contact the Federal Trade Commission for more information toll-free at 1-877-ID-THEFT (438-4338) (TTY: 1-866-653-4261), by email at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>, or writing to Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

A free copy of your credit report can be obtained from each of the credit bureaus once a year by going to <http://www.annualcreditreport.com> or calling 877-322-8228. Hearing impaired consumers can access TDD services at 877-730-4104. We encourage you to monitor these reports, as well as your credit and debit card statements. You may also place a fraud alert or security freeze on your credit report by contacting the credit bureaus as listed below.

| | | |
|--|---|---|
| Equifax P.O. Box 740241 Atlanta, GA 30374 888-766-0008 www.equifax.com | Experian P.O. Box 9554 Allen, TX 75013 888-397-3742 www.experian.com | TransUnion P.O. Box 6790 Fullerton, CA 92834 800-680-7289 www.transunion.com |
|--|---|---|

A security freeze will prevent new credit from being opened in your name without the use of a personal identification number or password that will be issued by the credit bureaus after you initiate the freeze.

A security freeze will also prevent potential creditors from accessing your credit report without your authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. In order to place a security freeze, you may be required to provide the credit bureaus 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. Credit bureaus may charge a fee up to \$10 to place, lift, or remove the security freeze; however, this fee may be less in certain states (in MA, up to \$5) or waived if you are the victim of identity theft and you provide a valid police report. You must separately place a security freeze on your credit file with each credit reporting agency.

Filing a Police Report for Suspicious Activity:

If you do find suspicious activity on the credit or debit card indicated in our notice to you or in your credit report, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. In addition, you should report identity theft to your Attorney General and the Federal Trade Commission.

For Maryland Residents: The Maryland Attorney General provides information regarding identity theft at <http://www.oag.state.md.us/idtheft/index.htm>. You may also contact the Identity Theft Unit at (410) 576-6491, by email at idtheft@oag.state.md.us, and by mail at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.