Table of Contents

We may be adversely affected by risks related to our dependence on IT systems. Any future intrusion into these IT systems, even if we are compliant with industry security standards, could materially adversely affect our reputation, financial condition and operating results.

We have complex IT systems that are important to the success of our business operations and marketing initiatives. If we were to experience failures, breakdowns, substandard performance or other adverse events affecting these systems, or difficulties accessing the proprietary business data stored in these systems, or in maintaining, expanding or upgrading existing systems or implementing new systems, we could incur significant losses due to disruptions in our systems and business.

Our ability to effectively manage the day-to-day business of approximately 900 Albertsons and NAI stores depends significantly on IT services and systems provided by SuperValu pursuant to two transition services agreements (the "SVU TSAs"). It is intended that SuperValu will also provide IT services and systems for the stores Acme Markets acquires pursuant to the A&P Transaction. Prior to Albertsons' and NAI's transition onto Safeway's IT systems, the failure of SuperValu's systems to operate effectively or to integrate with other systems, or unauthorized access into SuperValu's systems, could cause us to incur significant losses due to disruptions in our systems and business.

We receive and store personal information in connection with our marketing and human resources organizations. The protection of our customer and employee data is critically important to us. Despite our considerable efforts to secure our respective computer networks, security could be compromised, confidential information could be misappropriated or system disruptions could occur, as has occurred with a number of other retailers. If we (or through SuperValu) experience a data security breach, we could be exposed to government enforcement actions, possible assessments from the card brands if credit card data was involved and potential litigation. In addition, our customers could lose confidence in our ability to protect their personal information, which could cause them to stop shopping at our stores altogether. The loss of confidence from a data security breach involving our employees could hurt our reputation and cause employee recruiting and retention challenges.

Improper activities by third parties, exploitation of encryption technology, new data-hacking tools and discoveries and other events or developments may result in future intrusions into or compromise of our networks, payment card terminals or other payment systems. In particular, the techniques used by criminals to obtain unauthorized access to sensitive data change frequently and often cannot be recognized until launched against a target; accordingly, we may not be able to anticipate these frequently changing techniques or implement adequate preventive measures for all of them. Any unauthorized access into our customers' sensitive information, or data belonging to us or our suppliers, even if we are compliant with industry security standards, could put us at a competitive disadvantage, result in deterioration of our customers' confidence in us, and subject us to potential litigation, liability, fines and penalties and consent decrees, resulting in a possible material adverse impact on our financial condition and results of operations.

As merchants who accept debit and credit cards for payment, we are subject to the Payment Card Industry ("PCI") Data Security Standard ("PCI DSS") issued by the PCI Council. PCI DSS contains compliance guidelines and standards with regard to our security surrounding the physical administrative and technical storage, processing and transmission of individual cardholder data. By accepting debit cards for payment, we are also subject to compliance with American National Standards Institute ("ANSI") data encryption standards and payment network security operating guidelines. In addition, we are required to comply with PCI DSS version 3.0 for our 2015 assessment, and are replacing or enhancing our in-store systems to comply with these standards. Failure to be PCI compliant or to meet other payment card standards may result in the imposition of financial penalties or the allocation by the card brands of the costs of fraudulent charges to us. Despite our efforts to comply with these or other payment card standards and other information security measures, we cannot be certain that all of our (or through SuperValu) IT systems will be able to prevent, contain or detect all