



February 7, 2014

Consumer Financial Protection Bureau
Attention: Richard Cordray, Director
1700 G. Street, NW
Washington, DC 20552

RE: Retailer Data Breaches and Consumer Data Protection

Dear Director Cordray,

The Michigan Credit Union League & Affiliates (MCUL) is the statewide trade association representing 98% of the credit unions located in Michigan and their 4.6 million members. The MCUL appreciates the opportunity for open dialogue with the Consumer Financial Protection Bureau (CFPB) on regulatory and policy matters that impact Michigan's credit unions.

As a result of the recent high-profile, devastating security breach of the nationwide retailer Target, an estimated 70 million or more consumers have had their card and personal information compromised. The costs and resources associated with assisting these consumers and replacing potentially affected cards averages about \$5.10 per card, nationally resulting in a \$25-30 million impact for credit unions so far – not including any costs related to actual fraud that may result. In Michigan, credit unions have reported replacing thousands of cards for members, and Michigan credit unions have so far incurred over \$1.1 million in costs related to member assistance, fraud prevention, and recompense. Many have been forced to increase their staffing and extend their hours due to the significant increase in call volume and work associated with reissuance. Within the three days following the news of the Target breach, one Michigan credit union received over 7,000 member calls and identified approximately 22,000 affected accounts.

As an industry, we are just beginning to assess the impact, and MCUL fully expects these costs to increase as the industry learns more and any actual fraud occurs. Since the Target event, new breach events have come to light at other national retailers such as Neiman Marcus and Michael's. These events serve to shed further light on the problem that retailers are not implementing proper security protocols and care to protect the sensitive personal and financial information that they obtain from their consumers.

With this in mind, MCUL strongly urges the CFPB to engage in supervision of retailers that pointedly fail to take proper steps to protect consumers and their private information in the course of offering and providing consumer financial services. Consumers would certainly benefit from the regulation of a retail industry that, at the moment, relies on largely self-policing standards that are inadequate to the point of consumer deception, as illustrated by the often retroactive enforcement and revocation of certification with their tenets. MCUL believes that the Dodd-Frank Act's provisions regarding supervision of nonbank covered persons that engage in behavior that poses risks to consumers in this area provides clear authority for this supervision. The Dodd-Frank Act defines a consumer financial product or service, and under 12 U.S.C. 5481(15)(A)(v), an example of such is "selling, providing, or issuing stored value or payment instruments." Target offers both store-branded credit and debit options, and the debit option draws from customer's existing checking accounts. MCUL interprets these cards as "payment instruments" under the Dodd-Frank Act, therefore meeting the definition of a financial product. The protocols that a retailer puts into place (or fails to) in order to protect associated consumer personal and

financial information would certainly qualify as behavior that “poses risk to consumers with regard to offering or provision of [these] consumer financial products or services.” To the extent that CFPB requires complaints collected pursuant to federal law in order to initiate action, please consider this letter as one such, issued on behalf of Michigan’s 291 credit unions and all of our affected members.

Under 12 U.S.C. 5531 (Prohibiting Unfair, Deceptive, or Abusive Acts or Practices), the CFPB may take action to prevent a covered person or service provider from committing or engaging in an unfair, deceptive, or abusive act or practice in connection with a transaction with a consumer for a consumer financial product or service. The CFPB is permitted to take action if it has a reasonable basis to conclude that an act or practice causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable, and such injury is not outweighed by countervailing benefits to consumers or to competition. As further outlined by the CFPB, substantial injury usually involves monetary harm. An act or practice that causes a small amount of harm to a large number of people may be deemed to cause substantial injury.¹ MCUL would urge the CFPB to consider whether reliance on and promotion of a system of standards and certification or approval that by its very nature must change frequently to keep up with technology, and that may be re-determined retroactively following a negative event, paints an accurate and fair picture for consumers as to whether their critical personal data is really being protected by individual participants.

As I mentioned in a recent letter to the Michigan Congressional delegation, during the passage of Dodd-Frank, the “Durbin amendment” effectively shifted billions of dollars of interchange income from financial institutions into retailers’ pockets, with no meaningful price-relief or discernible consumer benefit having resulted. However, financial institutions still bear the brunt of the risk and the cost for a retailer’s lack of preparation and failure to adequately store and protect consumer data. This liability dynamic represents an arbitrary windfall that does nothing to encourage real reform or consumer protection, and cuts at financial institutions particularly hard – lost revenue, and lost wherewithal to pay for the sins of the retail community. It is time to bring shared accountability back into the equation for data breach liability.

MCUL believes that sufficient justification is provided under the Dodd-Frank Act for the CFPB to engage in the supervision and regulation of retailers that fail to protect client data, and to provide accountability and standards that will provide more meaningful consumer protection. In the coming weeks, MCUL looks forward to meeting with your staff during CUNA’s upcoming Government Affairs Conference, to further discuss this important endeavor to protect our members and provide them with the personal security that they deserve and rely upon.

Sincerely,



Dave Adams
President and CEO

¹ <http://www.cfpaguide.com/portalresource/Exam%20Manual%20v%202%20-%20UDAAP.pdf>