MICHIGAN CREDIT UNION LEAGUE & AFFILIATES

January 10, 2014

The Honorable Debbie Stabenow
United States Senator
133 Hart Senate Office Building
Washington, DC 20510

Re: Target Security Breach

Dear Senator Stabenow:

As you are well aware, the nationwide retailer Target was recently the subject of the latest, high profile devastating security breach and identity theft crime. As a result, estimates have stated that over 70 million credit cards may have been compromised during the holiday season. The attack appears to have focused on in-store, point-of-sale terminals as opposed to online sales operations, and questions surfaced in the immediate wake of the breach as to the efficacy of the retailer's security methods as well as internal and external data protection controls. While a complete investigation of the breach and what may have enabled it will likely take weeks if not months, sources have indicated that stolen card information and credentials have already flooded the "black market." This breach will likely affect many, if not all, card-issuing banks and credit unions, and their customers and members, across the country.

As we wait for further information to come to light, one thing is startlingly clear. Despite standards held up by the retail industry as protections for consumer data, industry self-policing and enforcement of such is inadequate and often retroactive. This becomes less startling, however, when one considers that it is the financial institution supporting the breached card, and not the retailer, that is often "left holding the bag" for the initial costs related to card replacement (including analysis and member communication) and the later cost of fraud itself. While they certainly endure risk to their reputation, as well as investigations and possible fines, the true cost of these crimes is born by financial institutions and their insurers that have little to no control over the actions, preparation, and protections utilized by the retailer.

In response to this latest breach, the Credit Union National Association (CUNA) and the Michigan Credit Union League & Affiliates (MCUL) will be gathering information on the specific effects that this incident has had on our credit unions and their members, from actual fraud to the costs associated with preventing it in a high risk situation. We will provide this information to you and your staff once it is collected, and we ask you to consider the equity of the current liability system. Why should financial institutions and their members continue to bear the brunt of the risk for a retailer's lack of preparation and failure to adequately store and protect consumer data? Shouldn't a retailer be held accountable for their own inadequate efforts, and shouldn't there be some recourse for those harmed that must ultimately

bear the costs involved? As you will recall, during the passage of Dodd-Frank, the "Durbin Amendment" shifted billions of dollars of interchange income from financial institutions into retailers' pockets, with no identifiable price-relief or benefit to consumers. The current liability dynamic represents yet another arbitrary windfall that does nothing to encourage real reform or consumer protection.

In the coming weeks, I look forward to discussing with you the costs that Michigan's credit unions and our members have been forced to endure as a result of this breach. I also look forward to a serious discussion about where the ultimate financial liability should rest for these incidents and what appropriate recourse options should be available, when retailer actions and "protections" do not measure up and entities downstream from the original compromised transactions are forced to take actions to protect themselves and their members and customers.

Sincerely,

David Adams
Chief Executive Officer