Written Statement of CVS Caremark

For

U.S. Senate Special Committee on Aging Hearing

"Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge"

July 16, 2014

Chairman Nelson, Ranking Member Collins and members of the Committee, CVS Caremark appreciates the opportunity to submit testimony for the hearing "Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge." CVS Caremark is committed to helping prevent scams when seniors enter our stores.

At approximately 7,600 CVS/pharmacy locations in the United States, we offer a variety of financial services and products, including wire transfers and reloadable prepaid cards. Given our extensive geographic footprint, these services and products provide consumers with a convenient option for paying bills; sending funds to friends and family; and budgeting for and tracking payments. For example, parents may choose to regulate and monitor a college-bound child's purchases by using a reloadable prepaid card rather than providing a credit card to the child. The overwhelming majority of these transactions at CVS/pharmacy locations are for legitimate purposes. As part of our anti-money laundering compliance program, we have implemented various controls to ensure that our products and services are not used for illegal purposes. These include daily transaction limits, identification requirements, colleague training, and monitoring for suspicious activity.

Despite these efforts, however, we are aware that a small percentage of our customers have been the victim of fraudulent scams carried out by criminals. These scams generally involve a perpetrator inducing the victim to wire funds or provide the "PIN" code of a prepaid product to the perpetrator. The perpetrator then transfers the victim's funds to another account, often leaving the victim humiliated and financially devastated. The scams are frequently targeted at senior citizens and prey on natural human instincts such as the desire to help a loved one in need. A common scam involves a call to a grandparent stating that his or her grandchild is in need of medical attention that cannot be provided until the grandparent sends funds.

In order to help our customers protect themselves from these scams, CVS Caremark has implemented the measures listed below in addition to the measures implemented by MoneyGram and the issuers of the prepaid products we sell. We continue to review and evaluate further opportunities to educate our customers about the risk of prepaid and wire transfer scams.

- **Training**. Annual training for our colleagues includes segments focused on consumer fraud and elder abuse. This training identifies some of the common scams of which we are aware and directs our colleagues to be on the lookout for red flags suggesting that a customer may be the victim a scam. If a colleague suspects a customer may be a victim of a scam, the colleague is directed to alert the customer to the risk of fraud and ask the

customer to reconsider the purchase. Periodically, we have reinforced this training through colleague awareness campaigns.

- **In-store warnings**. In CVS/pharmacy locations, we have posted warnings aimed at both customers using MoneyGram wire transfer service and customer purchasing prepaid products. For MoneyGram customers, we have affixed a sticker to the handle of the "red phone" that a customer must use to initiate a wire transfer that reads: "STOP. SCAM? Never send money to someone you don't really know." In addition, when the customer uses the phone to initiate a wire transfer, a fraud warning message is played in the language selected by the customer at the beginning of the call. (Similar warnings appear on the screen in the CVS/pharmacy locations where MoneyGram computer kiosks are located. For prepaid customers, we have posted signs in English and Spanish on the fixture where prepaid cards are sold warning customers of the risk of fraud. The sign reads: "PROTECT YOURSELF FROM SCAMS! Never send funds or share your PIN with someone you don't know – especially if contacted by phone. Don't scratch off the silver coating covering the PIN on the back of prepaid cards before purchase. To educate yourself about common scams or to report fraud, visit: http://www.fbi.gov/scams-safety/fraud."

- **Online warning**. On the page describing our financial services and products on www.cvs.com, we have included a banner alerting customers to the risk of scams and linking to www.scamawareness.org, a website operated by Scam Awareness Alliance, a non-profit organization dedicated to educating consumers about financial fraud.

These efforts have successfully prevented fraud in some cases. For example, an elderly Connecticut couple recently went to a CVS/pharmacy to purchase prepaid cards because they had been misled into believing their grandson was in police custody and directed to purchase prepaid cards to make a bail payment on his behalf. A CVS/pharmacy colleague warned the couple of the risk of scams, and the couple did not proceed with the purchase after confirming with the police that their grandson had not been arrested.

We commend our colleagues' actions in this and other similar circumstances, and we are pleased that we have been able to help some of our customers protect themselves from fraud. We are keenly aware, however, of the inherent limit on our ability as a retailer (1) to identify reliably all situations where a customer may be the victim of a scam; and (2) to persuade all customers who are the victim of fraud to reconsider the purchase.

Scams can involve a range of dollar amounts, and identifying whether a transaction is unusual for a particular customer can be a challenging and sensitive matter. Further, given the nature of these scams, shaking the victim's belief in the story spun by the scammer can be extremely difficult. Indeed, in one situation, a CVS/pharmacy colleague declined to sell a 93-year old customer several thousand dollars worth of prepaid cards and warned her of the risk of fraudulent scams. Despite this warning, however, the customer went to another retailer and purchased nearly $10,000 in prepaid cards.

Thank you again for the opportunity to submit testimony for the hearing “Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge.” We applaud the Senate Special Committee on Aging for focusing on this issue. We believe that educating consumers before they fall victim to a scam is the best way to reduce the incidence of financial fraud in this context, and we welcome any efforts to educate consumers, particularly the elderly, about the risk of scams.