Consumer Federation of America

FOR IMMEDIATE RELEASE
Thursday, Jan. 16, 2014

CONTACTS:
Susan Grant, CFA, 202-939-1003

DEALING WITH THE DATA BREACH EPIDEMIC

Consumer Education, ID Theft Protection Services are Not Enough

Washington D.C. – It seems that every week brings bad news about another data breach. The recent revelations about breaches at Target and Neiman Marcus have heightened concerns about the collection and security of consumers' personal information. "In this era of 'Big Data,' with an ever-increasing amount of information about individuals being amassed, there needs to be a stronger focus on data practices," said Susan Grant, Director of Consumer Protection at Consumer Federation of America (CFA). "It's not only in the business sector where people's data may be at risk," Grant said. "The massive breach at the South Carolina Department of Revenue in 2012 points to the need for better data practices by government agencies as well."

Grant noted that in the Target situation there are two problems; the theft of account numbers of credit and debit cards that consumers used at Target stores from November 27 through December 15, 2013, and the theft of consumers' names, addresses, phone numbers and email addresses, which was discovered when Target was checking its data systems in the wake of the account number breach. It is unclear how much overlap there is between these two data sets, but one thing is clear: millions of Target customers are potential fraud victims.

CFA recommends that consumers who used their credit or debit cards at Target stores during the specific time period involved should contact their card issuers to check for unauthorized transactions and ask for new account numbers. "Why wait to see if there is fraudulent activity on your account? Consumers should be proactive to protect themselves," Grant said. While consumers have limited liability for unauthorized charges and debits and most card issuers have adopted voluntary "zero liability" policies, dealing with fraud after the fact can be a hassle, especially for debit card holders whose bank accounts have been raided by crooks. Target says that debit card PIN numbers were encrypted, which makes it harder for the thieves to get into those accounts, but Grant advises that it is still a good idea to get new account numbers.

Another problem is the potential for "phishing" attacks against Target customers. This is when fraudsters pose as someone else that consumers may trust – in this case they might claim to be from Target, consumers' card issuers, an ID theft protection service, or a government agency investigating the breach – and ask for their personal information or direct them to click on something that plants malware in their computers or smartphones in order to steal their personal

information. Grant points out that phishing attacks could be carried out by the same crooks who hacked into Target's databases, or by others to whom they may have sold the data, or even by other crooks who simply take advantage of the news about the breach to contact consumers randomly, knowing that many may be Target customers. "If consumers get calls, letters, text messages or emails from anyone about the Target breach and asking for their personal information or directing them to do something, they should be very cautious," Grant warned. "Before responding, consumers should contact whoever the person claims to represent directly to confirm that the request is legitimate." She also suggests that rather than calling a number or going to a website that caller or sender provides consumers should look up the number or website independently.

Regarding Target's announcement that it is offering an ID theft protection service at no charge to all of its customers and has formed a coalition to launch a consumer education effort, Grant observed that that those measures, though welcome, are not enough. "The identity theft service that Target is paying for only monitors one of the three major credit bureaus and while it may alert consumers to new accounts opened in their names, it won't notify them about takeovers of their existing accounts or other types of identity theft, such as using their personal information to falsely obtain employment or tax refunds," Grant explained. "Consumers should also understand that the fraud assistance and insurance that will be provided are somewhat limited and that no ID theft protection service can prevent their information from being sold or used."

According to CFA, the most important thing that Target and others who hold consumers' personal information can do is improve their data practices. That includes not collecting more information than is needed for transactions, retaining data for only as long as necessary and hardening defenses against outside hackers and inappropriate internal access. "I'm not a security expert but clearly there needs to be greater commitment and more resources dedicated to security in order to fight this data breach epidemic," said Grant.

CFA provides information and links to resources about identity theft at www.IDTheftInfo.org and has tips and a video about phishing at www.consumerfed.org/fraud. Information from Target about its data breach and tips for customers is at www.target.com/databreach.

CFA is a non-profit association of nearly 300 consumer groups that was established in 1968 to advance the consumer interest through research, advocacy, and education.