SEATTLE--(BUSINESS WIRE)--Today consumers represented by law firm Hagens Berman Sobol Shapiro LLP filed a proposed class-action lawsuit against Target (NYSE: TGT) claiming the retail giant ignored warnings from as early as 2007 that the company's point-of-sale (POS) system was vulnerable to attack, a move that put millions of Americans' credit-cards and personal information at risk after the system was penetrated by unknown attackers on or about Nov. 17, 2013.

The lawsuit, filed by consumer-rights law firm Hagens Berman in the U.S. District Court for the Northern District of California, claims that security expert Dr. Neal Krawetz alerted Target and other major national retail chains about its vulnerability to attack in a white paper outlining POS vulnerabilities at major retailers. The paper warned that security shortcomings in POS systems could put the financial information of consumers at risk. The white paper used Target as a specific example of the potential impact, estimating that as many as 58 million consumers could be at risk of account theft unless the retailer took steps to fix the issues.

The complaint alleges that a Target developer responsible for the retailer's POS system was sent the white paper, acknowledged receiving it, and requested permission to send it to other Target employees. Attorneys claim that the developer also described Dr. Krawetz's suggestions as "good ideas." However, the lawsuit claims, Target ultimately failed to implement Dr. Krawetz's proposed security fixes, and thus remained vulnerable to the attack that followed several years later.

"We believe that Target not only knew its systems were vulnerable to exactly this kind of attack all the way back in 2007, but was alerted to and acknowledged suggestions that would have made its customers safer," said Tom Loeser, a Hagens Berman Partner and former federal prosecutor in the Cyber and Intellectual Property Crimes Section of the U.S. Attorneys' Office in Los Angeles. "However, Target did not act on this knowledge, and as a result, tens of millions have had their personal information stolen and financial accounts compromised."

The lawsuit also claims that Target was likely not compliant with industry standards for security, such as the PCI Data Security Standard ("PCI DSS"). For instance, the suit quotes an analyst who notes that three-digit CVV codes must have been stored in order for them to have been stolen, but storing CVV codes is a practice long banned by the PCI.

Attorneys allege that in addition to negligence prior to the security breach, Target repeatedly misled its customers about the nature and scale of the breach. For instance, the suit claims that Target initially stated that customers' PIN numbers were not compromised, but later disclosed that the data had, in fact, been taken. Attorneys also claim that Target initially estimated only 40 million accounts were affected, but later appeared to state that in addition to account information for 40 million charge cards, the personal information of 70 million customers was also compromised. Customers whose charge account information was compromised, and whose personal information, such as name, address, phone number, and email were also stolen, are at a heightened risk of identity theft, according to attorneys.

The lawsuit is a proposed class action, and seeks to represent a class of all persons in the United States who used a credit or debit card at a Target store and whose financial or personal information was compromised. It claims that Target's actions were negligent and additionally violated a number of state laws governing unfair business practices and the disclosure of security breaches.

"Following the data breach, Target acted consistently in its own self-interest and was not looking out for its affected customers," said Hagens Berman Managing Partner Steve Berman. "It did not disclose the data breach until a day after a private security blogger had discovered it, and even then it sought to minimize the effect the data breach would have on its holiday sales by disclosing the breach only on its corporate website and not disclosing that customer PIN numbers had also been stolen."

"The company should have immediately offered credit monitoring and/or identity theft protection for its customers and fully disclosed the potential risks," Mr. Berman continued. "Instead, Target instructed its customers to 'remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports.'"

"It is our hope," said Mr. Berman, "that this lawsuit will cause Target and other major retail chains that handle the personal and financial information of millions of Americans to take data theft seriously and continuously improve their security to meet the increasing threat from data breach attacks. Target chose to save millions by not implementing adequate data protection protocols, and we believe those savings should be used to compensate Target customers for the costs, frustration, and countless hours of lost

productivity that resulted."

Concerned consumers who made purchases at Target stores between Nov. 27, 2013, and Dec. 15, 2013 are encouraged to contact a Hagens Berman attorney by emailing Target@hbsslaw.com or calling (206) 623-7292.

Additional information about the investigation is available at http://www.hbsslaw.com/cases-and-investigations/cases/Target-Data-Breach .

About Hagens Berman

Hagens Berman Sobol Shapiro, LLP, is a consumer-rights class-action law firm with offices nine cities. The firm has been named to the National Law Journal's Plaintiffs' Hot List seven times. More about the law firm and its successes can be found at www.hbsslaw.com . The firm's class-action law blog is located at www.classactionlawtoday.com .