ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051

http://oversight.house.gov

November 12, 2014

Alasdair James
President and Chief Member Officer
Kmart Corporation
3333 Beverly Rd.
Hoffman Estates, IL 60179

Dear Mr. James:

I am writing to request information about a significant data breach recently reported by Kmart.

According to a report issued by Kmart on October 9, hackers breached the company's payment data systems in September "with a form of malware that was undetectable by current anti-virus systems."[1] Kmart reported that "certain debit and credit card numbers have been compromised" and that the breach may impact customers who made debit or credit card purchases in its U.S. stores in September and October.[2] Internet security investigative reports have suggested that "the information stolen would allow thieves to create counterfeit copies of the stolen cards."[3]

The increasing number of cyber-attacks and data breaches is unprecedented and poses a clear and present danger to our nation's economic security. Each successive cyber-attack and data breach not only results in hefty costs and liabilities for businesses, but exposes consumers to identity theft and other fraud, as well as a host of other cyber-crimes. Your ability to protect consumers and safeguard their personal information is central to earning and maintaining consumer confidence in our economic system.

The increased frequency and sophistication of cyber-attacks on both public and private entities highlights the need for greater collaboration to improve data security. Your company's knowledge, information, and experience with this recent data breach will be helpful as Congress examines federal cybersecurity laws and any necessary improvements to protect sensitive

---

[1] Kmart, *Kmart Investigating Payment System Intrusion* (Oct. 10, 2014) (online at www.kmart.com/ue/home/10.10.14_News_Release.pdf.).

[2] *Id.*

[3] Brian Krebs, *Malware Based Credit Card Breach at Kmart* (Oct. 10, 2014) (online at http://krebsonsecurity.com/2014/10/malware-based-credit-card-breach-at-kmart/).

consumer and government financial information. To aid in this oversight, I request that Kmart provide the following information:

(1) a description of the manner and method by which your company first discovered that its payment data systems were under cyber-attack in 2014;

(2) the approximate number of consumers that may have been affected by the breach;

(3) the findings from forensic investigation analyses or reports concerning the breach, including findings about vulnerabilities to malware, the use of data segmentation to protect personally identifiable information, and why the breach went undetected for the length of time it did;

(4) the individuals or entities suspected or believed to have caused the data breach, and whether they have been reported to the appropriate law enforcement agencies;

(5) a description of data protection improvement measures your company has undertaken since discovering that its payment data systems had been breached in 2014;

(6) an estimate of the number and value of fraudulent transactions that were connected to payment cards exposed in the data breach, including the approximate number of federal, state, and local government customers whose information was exposed during the data breach at issue, as well as the number and value of fraudulent transactions that were connected to payment cards from federal, state, and local government customers exposed in the data breach;

(7) a description of the data security policies and procedures that govern your company's relationships with vendors, third-party service providers, and subcontractors, including the manner by which your company ensures that entities performing work on your behalf have reasonable data security controls in place to thwart cyber-attacks; and

(8) any recommendations for improvements in cybersecurity laws or the coordination of efforts to identify and respond to emerging trends in cybersecurity risks to help prevent future data breaches.

Please provide the requested information by December 19, 2014. We also request a briefing from your Chief Information Security Officer or similar chief IT security professional by November 25, 2014. If you have any questions about this request, please contact Timothy D. Lynch at (202) 225-0312.

Thank you for your cooperation in this matter.

Sincerely,

Elijah E. Cummings
Ranking Member

cc: The Honorable Darrell E. Issa, Chairman