kmart

Frequently Asked Questions

What happened?
On Thursday, Oct. 9, 2014 our IT team detected that our payment data systems had been breached and immediately launched a full investigation working with a leading IT security firm.

Our investigation to date indicates the breach started in early September. According to the security experts we've been working with, our Kmart store payment data systems were infected with a form of malware that was undetectable by current anti-virus systems. We were able to quickly remove the malware. However we believe debit and credit card numbers have been compromised.

Based on the forensic investigation to date, no personal information, no debit card PIN numbers, no email addresses and no social security numbers were obtained by those criminally responsible. There is also no evidence that kmart.com customers were impacted. Given the criminal nature of this attack, Kmart is working closely with federal law enforcement authorities, our banking partners as well as leading IT security firms in this ongoing investigation.

What should customers know?
We sincerely apologize for any inconvenience this may cause our members and customers. We want our members and customers to be aware of the situation so they can take additional steps to safeguard their personal information. We suggest that customers carefully review and monitor their debit and credit card account statements. If customers see any sign of suspicious activity, they should immediately contact their card issuer. To further protect our members and customers who shopped with a credit or debit card in our Kmart stores during the month of September through yesterday (Oct. 9, 2014), Kmart will be offering free credit monitoring protection. The most up-to-date information will be available on our website, www.kmart.com.

Are you currently offering credit monitoring services to your Kmart customers?
Yes. All customers who shopped in Kmart's U.S. stores between Sept. 1, 2014 and October 9, 2014 may go to ProtectMyID.com/Kmart by April 15, 2015 and enroll in ProtectMyID for one year. Eligible individuals will need to confirm that they shopped with a credit or debit card at a Kmart store between September 1, 2014 and October 9, 2014. They will then be prompted to begin the enrollment process in the product. Members will receive an email confirming their enrollment for one free year (12 months) of ProtectMyID. Customers without web access can call 866-252-9553 to enroll over the phone.

What steps should I take to protect my information?
As a rule, it always makes good sense to review your credit card and banking statements regularly and immediately report suspicious activity to your bank or card issuer. The policies of credit card companies normally state that you are absolutely not responsible for fraudulent activity on your payment cards when you report that activity in a timely manner. The most up-to-date information will be available on our website, www.kmart.com.

Is it safe to shop at Kmart?
Yes. Our members and customers are very important to us. We take the safety and security of our customers' private information very seriously. Our IT teams quickly removed the malware and we are

deploying further advanced software to protect our customers' information. And it's important to note based on the forensic investigation to date, no personal information, no debit card PIN numbers, no email addresses and no social security numbers were obtained by those criminally responsible.

When did the data breach first occur?
Our investigation to date indicates the breach started in early September 2014.

When did you discover this?
On Thursday, Oct. 9, 2014 our IT team detected that our payment data systems had been breached and immediately launched a full investigation working with a leading IT security firm.

Were any Sears, Roebuck customers impacted?
No. Our preliminary investigation has found that this malware infected the payment data systems at Kmart stores only. It has been contained and removed. We sincerely apologize for any inconvenience this may cause our members and customers.

Were customers who made purchases on Kmart.com impacted?
No. Our preliminary investigation has found that this malware infected the payment data systems at Kmart stores only.

What steps is Kmart taking regarding this payment data system breach?
First and foremost we're communicating with our Kmart customers to keep them informed as our investigation continues. To further protect our members and customers who shopped with a credit or debit card in our Kmart stores during the month of September through yesterday (Oct. 9, 2014), Kmart will be offering free credit monitoring protection.

Given the criminal nature of this attack, Kmart is working closely with federal law enforcement authorities, our banking partners and IT security firms in this ongoing investigation. We are deploying further advanced software to protect our customers' information.

Did the hackers take customers' debit card PINs, too?
Based on the forensic investigation to date, no personal information, no debit card PIN numbers, no email addresses and no social security numbers were obtained by those criminally responsible. In addition, a significant percentage of Kmart store customers pay for transactions with cash.

What information was stolen?
We believe debit and credit card numbers have been compromised. Based on the forensic investigation to date, no personal information, no debit card PIN numbers, no email addresses and no social security numbers were obtained by those criminally responsible. According to the security experts we've been working with, our Kmart store payment data systems were infected with a new form of malware that was undetectable by current anti-virus systems. We were able to quickly remove the malware.