kmart

Frequently Asked Questions

1) Has Kmart experienced a recent data breach?
We recently became aware of a security incident in which Kmart was a victim of unauthorized credit card activity following certain customer purchases at some of our Kmart stores. We immediately launched a thorough investigation and engaged leading third party forensic experts to review our systems and secure the affected part of our network.

Our Kmart store payment data systems were infected with a form of malicious code that was undetectable by current anti-virus systems and application controls. Once aware of the new malicious code, we quickly removed it and contained the event. We are confident that our customers can safely use their credit and debit cards in our retail stores.

Based on the forensic investigation, NO PERSONAL identifying information – including names, addresses, social security numbers, birth dates and email addresses – was obtained by those criminally responsible. However, we believe certain credit card numbers have been compromised. All Kmart stores were EMV "Chip and Pin" technology enabled during the time that the breach occurred, and we believe the exposure to cardholder data that can be used to create counterfeit cards is limited. There is no evidence that kmart.com or Sears customers were impacted nor that debit PIN numbers were compromised.

2) Has DOJ, FBI or any law enforcement agencies reached out to you about a data breach?
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 cannot comment on any specific activities by those counterparties; please direct those questions to them.

3) Have law enforcement, banks, processors, credit card companies or anybody else warned Kmart about unusual fraudulent activity coming from cards used at Sears? In past six months?
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 cannot comment on any specific activities by those counterparties; please direct those questions to them.

4) Have you hired an outside forensics firm to investigate whether there was a breach or is currently a breach in POS or other parts of your network? What status of that investigation?
Yes, we immediately launched a thorough investigation and engaged leading third party forensic experts to review our systems and secure the affected part of our network. We have removed the malicious code and contained the event. We are confident that our customers can safely use their credit and debit cards in our retail stores.

5) Have you lost any other types of customer data to hackers (like the info in your customer loyalty card database)?
Based on the forensic investigation, NO PERSONAL identifying information – including names, addresses, social security numbers, birth dates and email addresses – was obtained by those criminally responsible.

All Kmart stores were EMV "Chip and Pin" technology enabled during the time that the breached had occurred and we believe the exposure to cardholder data that can be used to create counterfeit cards is limited. There is no evidence that kmart.com or Sears customers were impacted nor that debit PIN numbers were compromised.

6) We understand that Kmart is investigating potential POS breach at multiple stores. Is that accurate?
We recently became aware of a security incident in which Kmart was a victim of unauthorized credit card activity following certain customer purchases at some of our Kmart stores. We immediately launched a thorough investigation and engaged leading third party forensic experts to review our systems and secure the affected part of our network.

Our Kmart store payment data systems were infected with a form of malicious code that was undetectable by current anti-virus systems and application controls. Once aware of the new malicious code, we quickly removed it and contained the event. We are confident that our customers can safely use their credit and debit cards in our retail stores.

7) Are you re-assessing your data security systems to determine a breach? Are you considering an overhaul or keeping what you have in place?
Data security is of critical importance to our company. We maintain appropriate and reasonable physical, electronic, and procedural security safeguards to protect our data, and we continuously review and improve those safeguards in response to changing technology and new threats. We are actively enhancing our defenses in light of this new form of malware, but it is our policy not to discuss the specific details of our security measures.

8) Would you notify the members if their data has been compromised?
We are complying with all applicable legal requirements and working with the payment card networks to notify the card-issuing banks who maintain the contact information for customers whose cards may have been impacted.

Based on the forensic investigation, NO PERSONAL identifying information – including names, addresses, social security numbers, birth dates and email addresses – was obtained by those criminally responsible.

All Kmart stores were EMV "Chip and Pin" technology enabled during the time that the breach occurred and we believe the exposure to cardholder data that can be used to create counterfeit cards is limited. There is no evidence that kmart.com or Sears customers were impacted nor that debit PIN numbers were compromised.

9) Is there any link to previous breach? Would you say that you did not completely eradicate the threat identified in previous attacks?
We do not believe that this recent attempt has any link to a previous security event.

10) What are you doing to make sure that it doesn't happen again?
Data security is of critical importance to our company. We continuously review and improve the safeguards that protect our data in response to changing technology and new threats. We are actively enhancing our defenses in light of this new form of malware, but it is our policy not to discuss the specific details of our security measures.

11) Has any of the Shop Your Way or Sears' customer data been compromised?
There is no evidence that Shop Your Way or Sears customers were impacted.

12) Is the company able to make the appropriate investment to protect member and PCI data?
Data security is of critical importance to our company. We continuously review and improve the safeguards that protect our data in response to changing technology and new threats.

13) Why have you not gone public if you believed your systems have been compromised?
We do not comment on or discuss ongoing investigations.

14) Are you offering credit monitoring services?
No. NO PERSONAL identifying information was obtained, our POS systems are EMV compliant, and we believe cardholder data exposure that can be used to create counterfeit cards is limited.