

# Inquiry launched after biggest ever credit card heist

- Raids on fashion retailer TK Maxx in US and UK
- 45 million at risk on both sides of Atlantic

**Rebecca Smithers and Bobbie Johnson**  
**Saturday March 31, 2007**

## **Guardian**

British authorities yesterday launched an inquiry into how computer hackers who targeted the cut-price fashion retailer TK Maxx were able to steal information from more than 45 million credit and debit card holders on both sides of the Atlantic.

As the extraordinary scale of the biggest credit card heist unravelled, internet security experts urged all businesses and banks to tighten up their computer security systems to protect their customers.

TK Maxx shoppers were advised to check their credit and debit transactions for irregularities amid warnings that the criminals involved could even use the data to commit identity theft. Internet fraud is now one of the fastest growing areas of illegal activity in the UK.

TK Maxx's US parent company, TJX, revealed the extent of the "unauthorised intrusion" in its annual report on Thursday, claiming that someone had used sophisticated software to access its data centres in Watford, Hertfordshire, and in Framingham, near Boston, Massachusetts.

Names, card numbers and personal data were stolen - and in the US, social security numbers - over a 17-month period and covering transactions dating as far back as December 2002. The firm said it did not know how many of the cardholders affected were shoppers at TK Maxx's 210 stores in Britain and Ireland, although more of them were likely to be American. Canadian shoppers have also been affected. The company disclosed in January that it had a problem but suggested the volume of information stolen was not on a large scale.

The government's information commissioner, Richard Thomas, was said to be extremely concerned. A spokesperson for his office said yesterday: "The information commissioner's office takes breaches of privacy extremely seriously. The Canadian privacy commissioner is investigating this matter and is working with the federal trade commission in the US. We are liaising with them on this. It was brought to our attention today that information may have been hacked from the company's data centre in Watford. We are therefore contacting the company in the UK today. To date we have not received any complaints arising from this breach."

Crime of this type is common, and £210m was lost to credit card fraud during the first half of 2006, according to figures from the payment industry body Apacs. But some experts say fraud and hacking is at far greater levels than realised.

"We see a couple of commercial thefts at a very serious level each week," said Dan Hagman of 7 Safe, which specialises in so-called intrusion forensics. "Credit card details are being stolen in huge numbers - and the problem is that if you're hacked you don't necessarily know."

Although it remains unclear how many of TK Maxx's customers have been defrauded as a result of the security failure, Mr Hagman said the impact of an investigation by the information commissioner would be unprecedented: "This is not a little site, it's a big, well-respected player and I think this case is going to have a profound effect on how the industry deals with security."

David Hill, ID theft specialist at the personal security company red24, said: "People should most definitely be concerned, and if they have shopped in TK Maxx they should go back through their credit card and bank statements to make sure no fraudulent transactions have taken place. Criminals carrying out credit card fraud will often make small purchases as these are less likely to stand out and may go undetected. If people do spot suspect transactions ... they should immediately shut down their accounts and any linked accounts and register with a credit reference agency."

New legislation coming into force in June will impose tough penalties and sanctions on companies that fail to safeguard their customers' card information.

British consumers should ring **0800 779 015** and those in the Republic of Ireland **0044 800 77915**. The homepage at [www.tkmaxx.com](http://www.tkmaxx.com) has a customer alert with updated information.

## **FAQ: TK Maxx**

### **When did this happen?**

According to TK Maxx, the intrusions began in July 2005 and cover credit and debit card purchases stretching back to 2003. The hacking activity ended in December 2006, which is likely to be the first time the company became aware of a problem. It admitted the breach in January, but it was only this week that the full extent of the problems was revealed.

### **Why did the problems last so long?**

In most cases, a company discovering a security breach will act to close down the loophole that lets hackers in immediately. However, it is quite possible that criminals could have been operating invisibly for almost 18 months before being discovered.

### **Why did they keep details on file?**

There are no strict rules on how long transaction data can be held, and guidelines from Britain's privacy watchdog suggest it can be kept for as long as there is a "business use".