



- [MSNBC Home](#)
 - » [Technology & Science](#)
 - » [Security](#)
 - » [The Red Tape Chronicles](#)



About this blog



Corporate sneakiness. Government waste. Technology run amok. Outright scams. The Red Tape Chronicles is MSNBC.com's effort to unmask these 21st Century headaches and offer real solutions that save you time and money.

Bob Sullivan covers Internet scams and consumer fraud for MSNBC.com. He is the winner of multiple journalism awards for his coverage of online crime and author of [Gotcha Capitalism: How Hidden Fees Rip You Off Every Day and What You Can Do About It](#). and [Your Evil Twin: Behind the Identity Theft Epidemic](#).

Got some red tape you want Bob to untangle? Write BobSullivan@feedback.msnbc.com.

Credit card

hackers find new, rich targets

Posted: Friday, January 23 at 05:00 am CT by Bob Sullivan

Few noticed on Christmas Eve when the news broke that electronic payment services firm RBS WorldPay had been hit by hackers who stole personal data on 1.5 million consumers. After all, that's small potatoes these days. But when Heartland Payment Systems announced on Inauguration Day that it had suffered a serious security breach, some experts noticed a pattern -- and not just the companies' standard penchant for releasing bad news on days while the public is distracted.

"I have heard that the payment processors are the main target for hackers now," said Avivah Litan, security expert at consultancy firm Gartner.

Heartland has not released an estimate of the number of accounts impacted by the attack, but Litan said it might be the biggest data leak ever: The firm handles 100 million transactions every month for 250,000 clients. Heartland has said it was alerted by Visa and MasterCard to a pattern of fraud on its networks last fall, but only discovered the security hole in its network last week. That gave hackers access to potentially hundreds of millions of transactions over several months.

The largest known data leak to date involved retailer TJ Maxx, which lost the data on 45 million credit cards in 2007. But this time, there are signs the haul, and the targets, might be astonishingly large.

In its release, Heartland said it was the victim of a "widespread global cyber fraud operation." CFO Robert Baldwin told the Wall Street Journal that the firm had been targeted by malicious software that was "light-years more sophisticated" than standard computer viruses. Those ominous statements, combined with the news about RBS WorldPay, suggests to Litan that hackers have now trained their relentless keyboards on payment processing firms.

Few American consumers have ever heard of Heartland or RBS WorldPay. But these firms -- and others including First Data, TSYS, and Nova Information Systems -- regularly capture and transmit personal information about nearly every American.

Payment processors handle credit-, debit- and gift-card transactions from the moment you swipe your card at a store until your bank debits your account and adds the money to the store's account. These are complicated processes -- the processor must make sure you have the money (or the credit limit) to afford the purchase, then tell your bank to send money to the store's bank. Often, third-party firms -- such as software companies that manage store cash registers -- add to the complexity.

Right now, consumers have no way of knowing if their data was stolen RBS WorldPay or the Heartland attacks; they may never find out. Retailers rarely advertise which payment systems they use. Heartland has said publicly that nearly half of its transactions come from restaurants, but has declined to identify its clients. It's also declined to identify consumers who might be victims.

That's where the data is

It makes sense for hackers to target processing companies -- that's where the most data is. A firm like Heartland has access to far more credit and debit card numbers on a given month than any single retailer. But there's another factor that makes processors vulnerable, Litan said. While payment industry rules require that credit card data be encrypted while it's stored by retailers, processors, and banks, there is no requirement that the data be encrypted while in transit over private networks. That's a weakness which hackers have now targeted, she said.

Heartland isn't saying how a computer virus was able to get onto its systems. But once there, its makers would have had a fairly easy time sniffing out credit card data, Litan said.

"The likelihood is that there was malicious software sitting on a server (at Heartland) looking for transmissions that represented authorization requests, and then the malware would turn on and capture that data," she said.

In August of last year, Visa issued a warning to payment services companies predicting exactly that kind of attack.

"Visa has noticed an emerging trend in which computer hackers use packet sniffers to intercept and collect cardholder data," it said in a security alert sent to clients. "Recent investigations have uncovered evidence of packet sniffers being used by network intruders to capture payment card data as it is transmitted over the network during authorization. This threat involves compromising the system and then installing a sniffer program or installing a hardware sniffer. ... Once network intruders gain entry into a merchant's system, the packet sniffer programs are installed and can be difficult to detect."

Adding encryption tools would foil such packet sniffing, but doing so is a logistical challenge; all the various parties would have to agree on encryption key management. Still, Litan said, such a step would not be impossible -- and she criticized banks as "lazy" for not requiring encryption.

"They could do it. It's just very costly," she said.

Then again, so is a major security breach.

Leave a comment below or become a member of the [Red Tape Raiders and be a consumer advocate!](#)



[Main page](#)