

[TechNewsWorld](#) > [Security](#) > [Internet Fraud](#) | [Read Next Article in Internet Fraud](#)

November 27, 2007 12:16:26 PM

Please note that this material is copyright protected. It is illegal to display or reproduce this article without permission for any commercial purpose, including use as marketing or public relations literature. To obtain reprints of this article for authorized use, please call a sales representative at (818) 461-9700 or visit <http://www.ectnews.com/about/reprints/>.


Report: E-Commerce Fraudsters' Haul May Reach \$3.6B in 2007




By Erika Morphy
[E-Commerce Times](#)
Part of the ECT News Network
11/19/07 2:48 PM PT

[Back to Online Version](#)
[E-Mail Article](#)
[Digg It](#)
[Reprints](#)

Not surprisingly, merchants are employing more antifraud tools on their e-commerce sites. One possible -- and unwelcome -- result is a slowdown in response to legitimate customer orders. Twenty-seven percent of orders were manually reviewed in 2007, compared to 23 percent the year before; the number of orders requiring manual processing is growing faster than online sales.

It is becoming increasingly unsafe to buy or otherwise conduct business  online, according to the ninth annual [CyberSource](#) survey on e-commerce fraud.

Fraudsters will divert approximately US\$3.6 billion from U.S. e-commerce in 2007, a 20 percent increase over 2006, based on survey results.

Merchants are working aggressively to hold back the tide. Their various online security products and related best practices are keeping the [fraud](#) rate stable, notes CyberSource (Nasdaq: CYBS) . Still, it's requiring the expenditure of more resources to keep fraudsters at bay.

Survey participants estimated that 1.4 percent of their [online](#) sales this year will be diverted to illegitimate sources -- the same percentage as last year. However, that's 1.4 percent of a far higher volume of sales. That translates into dollar losses equal to \$3.6 billion in goods and services this year, up from \$3.1 billion in 2006.

"eCommerce in the U.S. today is a highly rewarding channel that is showing vigorous growth," noted Doug Schwegman, CyberSource director of customer and market intelligence, "but it's also a channel with meaningful challenges posed by systematic fraud."

More Tools, More Frustration

Not surprisingly, merchants are employing more antifraud tools on their e-commerce sites. These include order velocity monitoring, which detects suspicious purchase patterns, and IP geolocation, which can help pinpoint the physical point of origin of an Internet order, according to CyberSource.

In 2007, 53 percent of merchants surveyed used five or more fraud detection tools, with the largest merchants using an average of eight. One possible -- and unwelcome -- result is a slowdown in


response to legitimate customer orders.

Twenty-seven percent of orders were manually reviewed in 2007, compared to 23 percent the year before, CyberSource found. With online sales growing at about 20 percent per year, the number of orders requiring manual processing is growing faster than online sales. Approximately 38 percent more orders were reviewed in 2007 than in 2006, CyberSource estimates -- and that extra diligence may have cost merchants an extra \$100 million.

The perception that the Internet is not safe has taken a toll on e-commerce activity.

"We know from research that we've conducted through third parties in the U.S. that one of the elements that drives consumers away from online purchases is related to fraud and security," Pragnesh Shah, CEO of Mobilians, told the E-Commerce Times. "When we talk to parents of young people online, aged 14 to 18 years old, we know that kids are making purchases using their parents' credit and debit cards. These parents are concerned with getting phished or pharmed. ... This is reality."

Getting Worse

It's unlikely the problem will abate in the foreseeable future. Phishing itself, for instance, is no longer seen as a major money pot, Andrew Klein, senior product marketing  manager with SonicWall, told the E-Commerce Times. The real moneymakers are the phishing tools that are continuously being developed and deployed.

Attacks on corporations also appear to be gaining momentum. "The notion of corporate phishing is not new -- hackers have played with it in the past. The problem was, they didn't know how to monetize it, so they didn't pay that much attention to it," Klein said. That appears to be changing as more firms are targeted for their customers' information.

There may be a bright side, though.

More customers are focusing on [data](#) encryption as a privacy best practice, Luis Salazar, a partner in the data privacy and security law taskforce at Greenberg Traurig, told the E-Commerce Times.

"I think word has gotten around that encrypting your data is the best way to avoid problems under data breach laws, so many businesses are taking advantage of this," he said. Also, "there have been so many news stories -- often on the local evening news -- about records simply dumped 'out back' that businesses have started to take notice. They are now making sure to properly discard their data."

With hackers apparently lurking everywhere, securing offline channels has become essential too. 

▶ **Next Article in Internet Fraud: [Fighting Phishing](#)**

Related Resources

- [Podcast: Medical Network on the Move - Administering Employee Medical Testing Requirements ...](#)
- [EMBASSY Key Management Server: Trusted Computing Key Management](#)
- [Web Services: Insurers Gear up for Implementation](#)
- [CMiC Enterprise - ERP For Construction and Engineering](#)

Copyright © 1998-2007 ECT News Network, Inc. All Rights Reserved. See [Terms of Use](#) and [Privacy Policy](#). [How To Advertise](#).