

SAVVY SOLUTION PROVIDERS ARE BEATING BACK WOULD-BE SCAMMERS WITH TOUGH NEW ANTIFRAUD MEASURES AND THE HELP OF DISTRIBUTORS AND RESELLER ORGANIZATIONS

Crime Scene

By [Steven Burke](#), ChannelWeb



3:34 PM EDT Fri. Sep. 17, 2004

From the September 20, 2004 issue of CRN

At least once a day, solution provider CompSource finds itself the target of a ripoff artist. In fact, Dean Bellone, founder and CEO of the \$12 million, 13-year-old Cleveland-based company, has been targeted so many times he now considers himself a fraud expert.

The way Bellone sees it, if, like CompSource, you do about 65 percent of your sales over the Internet and you want to stay in business, you'd better learn how to outfox the bad guys. "If every one of those hit, we wouldn't be here," he said. "A lot of companies hit by these scams end up dying off. It's very discouraging."

What's also troubling to Bellone and other solution providers is the sharp spike in credit card fraud and Internet scams they've seen in the past year. A CRN Online Quick Poll last week found that 82 percent of all solution providers surveyed are seeing an increase in credit card scams and Internet fraud. What's more, 49 percent said these practices are up more than 100 percent in the past year.

Solution providers are fighting back with tough security measures and new policies for their sales reps, including refusing to ship out of state or out of the country ([see chart below](#)). They're also turning to a new class of vendors that offer identity verification products and services.

The rise in these crimes has put distributors and reseller organizations on the offensive, monitoring orders and implementing proactive campaigns to help prevent their solution provider customers from being scammed.

ASCII Group members, for example, use the national reseller organization's online forum to alert one another to scams. Risa Stolly, CEO of A-Prompt, a Lehigh Valley, Pa., solution provider, halted an out-of-state Internet order earlier this year after enlisting another ASCII member to check out the customer address. The fellow solution provider drove to the address listed and discovered it was a vacant lot.

Solution providers say strong measures are needed now more than ever, especially since they have had little luck getting help from local law enforcement and federal authorities in tracking down and prosecuting the scammers.

The costs of letting your guard down can be enormous, said Bellone. If the daily instances of attempted fraud at CompSource were successful, he said, his company would be out about \$20,000 a month. This summer, Bellone said CompSource was the target of an even larger scam—a complex sting operation by a con artist representing a bogus phone company with a \$1 million-plus order for computers supposedly headed for Iraq to help in the U.S. rebuilding effort. Bellone smelled a scam and hired a fraud specialist ([see sidebar](#)) who quickly discovered the company was fake and its executive had a serious rap sheet. "That would have been our demise," said Bellone. "Believe me, it was incredibly tempting. The old adage is true: If it seems too good to be true, it probably is."

Solution providers say the ripoff artists are using a variety of scams to hide their true identities. Some simply send requests for price quotes from free e-mail addresses such as yahoo (NSDQ:[YHOO](#)).com or hotmail.com; others use hearing-impaired relay communications services such as TTY or TDD. Payment is made with bogus checks or phony credit card numbers.

Then there is an increasing amount of more complex frauds that involve things like "bust-out scams," in which the solution provider's confidence is gained over time with small orders that are paid promptly before the scammer places a much larger order and then skips out on it. Some scammers even acquire legitimate businesses to use as a front to order hundreds of thousands of dollars of equipment and then close up shop, fleeing with the goods.

The credit card scams are hitting smaller solution providers harder than enterprise solution providers, since they usually involve orders for quickly disposable commodity items such as memory, toner cartridges, laptops or even Cisco Systems (NSDQ:[CSCO](#)) routers.

Investigators and fraud specialists agree that inexperienced and new solution providers are prime targets. They also say the sluggish IT sales environment is causing some otherwise-savvy solution providers to jump at the credit card offers or cons. "Someone that is new or is hurting for sales will bite on these," said Jay Tipton, CEO of Technology Specialists, a 21-year-old Fort Wayne, Ind., solution provider and ASCII Group member. Tipton said he's faced with at least one case of attempted fraud each day, up from one about every three months a year ago.

Technology Specialists does very few Internet orders, but when it does accept them the solution provider requires a fax-back form, credit card check with address verification, and an envelope sent to that location with a recent postmark to ensure it's legitimate.

Distributors, meanwhile, are on the job helping solution providers protect themselves by monitoring orders and flagging suspicious activity.

Tech Data (NSDQ:[TECD](#)), for one, has stopped a number of fraudulent orders and logged some 300 cases this year involving credit card scams, said Daniel Dunn, vice president of loss prevention and security at Tech Data. The Clearwater, Fla., distributor has issued fraud alerts, red flags and best practices to assist its solution providers, said Dunn. "You have zero protection on an Internet sale," cautioned Dunn. "You will be charged back if it is a stolen credit card. We want to protect our customers."

Ingram Micro (NYSE:[IM](#)) flags an estimated 300 orders a day as potential fraud, of which approximately 1 percent are verified as fraudulent by an Ingram Micro security specialist. Robert Burbach, vice president of worldwide security at Ingram Micro, Santa Ana, Calif., said preventing fraud is more "art than science" and requires information sharing and staying on top of the rapidly changing scams.

D&H Distributing is also battling the increasingly ingenious con artists by devoting a portion of its Web site to detailed information on how to avoid the scams. "We have a whole team on this," said Dan Schwab, vice president of marketing at the Harrisburg, Pa., distributor.

Howard Petrick, president of Noe Valley Computers, a 16-year-old San Francisco-based solution provider, is someone who has benefited from decisive action by his distributor, in this case Tech Data. Earlier this month, Petrick placed an order for \$8,000 of memory that was taken via a hearing-impaired telephone service and paid for with a credit card that cleared the issuing bank's fraud department. However, a Tech Data investigator stepped in when Petrick placed a similar order for \$8,900 of hard drives from the same client the very next day. Tech Data confirmed the order was a fraud and notified FedEx, which dispatched a security officer who was able to recover the equipment from someone getting ready to reship it overseas.

Petrick feels older and wiser now that he has been stung. "I have done a lot of work overseas, and this is the first time anything like this has happened to me," he said. "I'll be more cautious and start looking more closely at larger orders, particularly with someone we have not done business with [before]." What burns Petrick is that on this particular order the credit card issuer authorized the transaction. "I thought once the credit card cleared I didn't have to worry," he said.

A-Prompt's Stolly said a simple way to avoid problems is to know your customer. "Many of us have a core set of customers that we deal with on a regular basis," said Stolly. "If you get someone outside of that group, look at them a little more closely."

CompSource's Bellone has found some success with a warning cautioning prospective buyers before they make an Internet purchase that CompSource prosecutes fraud to the fullest extent of the law. He has also cut down on a significant amount of potential problems by using Verid's VerID service, which verifies identity with multiple choice questions. That service, which CompSource implemented eight months ago, has had nearly a 100 percent track record ferreting out fraudulent orders, said Bellone.

But Bellone is most excited about the prospect of implementing CardinalCommerce's secure payment service, which he is now beta testing. "This is a huge breakthrough," said Bellone. "It's a minimal fee per month and a small transaction fee for the only system that makes the issuing bank liable."

Bellone says he is hopeful the new technology will help close the door on fraud activity. "It seems to me that technology is finally catching up where you are not going to have to rely as much on intuition," he said.

Jason Spotz, a CompSource accounts manager who has a perfect five-year track record ferreting out fraudulent orders, is not so sure. He says scamming is at an all-time high and it is sometimes nothing more than a hunch that causes him to pull back an order. "It's something you sometimes can't teach," said Spotz, estimating he has stopped a half-million dollars in fraudulent shipments. "It's gotten a lot worse with more people buying online. It's easier to steal someone's identity and rob someone online rather than using a gun and going in and robbing a store."