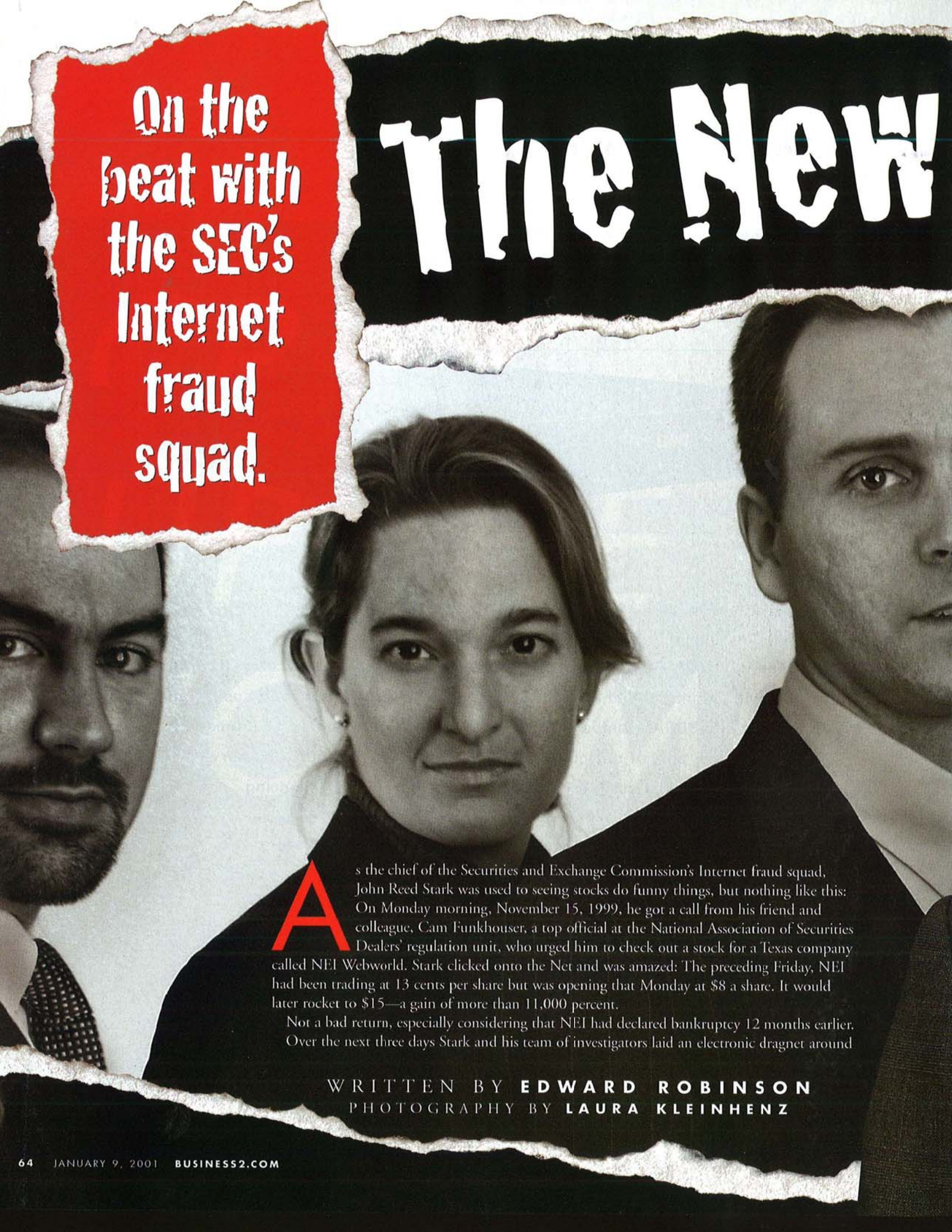
The New

On the beat with the SEC's Internet fraud squad.

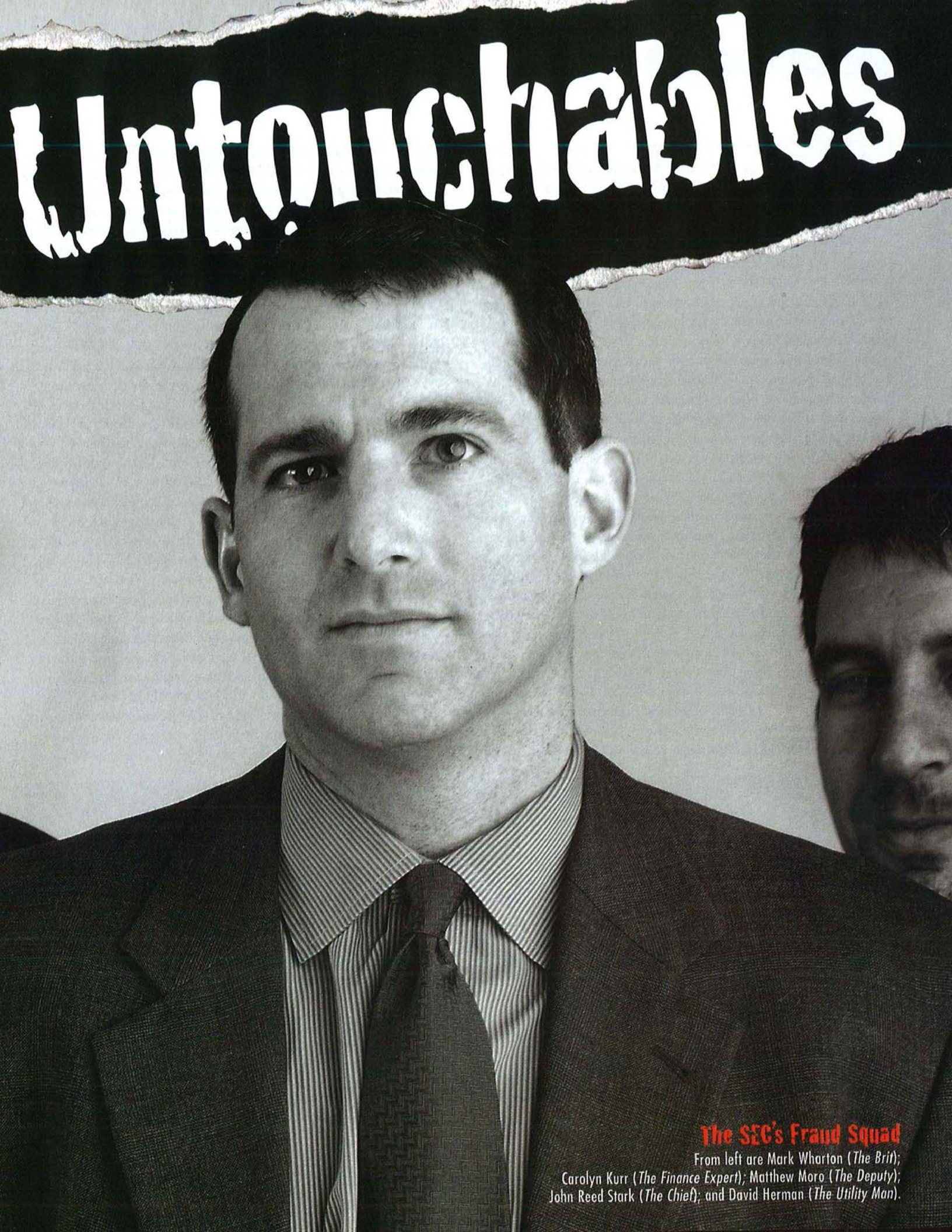


As the chief of the Securities and Exchange Commission's Internet fraud squad, John Reed Stark was used to seeing stocks do funny things, but nothing like this: On Monday morning, November 15, 1999, he got a call from his friend and colleague, Cam Funkhouser, a top official at the National Association of Securities Dealers' regulation unit, who urged him to check out a stock for a Texas company called NEI Webworld. Stark clicked onto the Net and was amazed: The preceding Friday, NEI had been trading at 13 cents per share but was opening that Monday at $8 a share. It would later rocket to $15—a gain of more than 11,000 percent.

Not a bad return, especially considering that NEI had declared bankruptcy 12 months earlier. Over the next three days Stark and his team of investigators laid an electronic dragnet around

WRITTEN BY **EDWARD ROBINSON**
PHOTOGRAPHY BY **LAURA KLEINHENZ**

Untouchables



The SEC's Fraud Squad

From left are Mark Wharton (*The Brit*); Carolyn Kurr (*The Finance Expert*); Matthew Moro (*The Deputy*); John Reed Stark (*The Chief*); and David Herman (*The Utility Man*).

NEW UNTOUCHABLES

Reverse merger
A transaction in which a privately held company "goes public" by acquiring a controlling block of a public company's equity and assuming the company's ticker symbol. In a normal merger it is a public company, using its stock as acquisition currency, that does the buying.

the stock and eventually tracked the trades to three people, including a pair of former students of the University of California at Los Angeles. They had manipulated NEI's lifeless security by sending hundreds of spams to message boards on Yahoo!, Raging Bull, and other investing sites claiming that NEI was about to be acquired in a reverse merger by a private, San Jose, Calif., firm called LGC Wireless.

The claim was a complete fabrication, of course, but it worked: The culprits pocketed more than $360,000 in profits. They didn't have much time to savor their success: A few weeks later the SEC obtained a court order to freeze their assets, and the FBI arrested the two worst offenders. It was one of the first major cases Stark's unit broke open that involved message-board spam—a favored MO of online stock swindlers.

While it's no secret that the Net's reach and get-rich-quick ethos has presented stock swindlers with a mammoth opportunity to perpetrate scams like these, what is far less known is exactly how the Feds have mobilized to fight them. The SEC's Internet fraud squad, started by one man with an idea and an America Online account, made almost 100 cases last year—up from five just four years ago.

Keeping up with the workload hasn't been easy. The explosion of online trading—three out of every 10 trades are now executed online, estimates Chase H&Q—and the oceans of investing information on the Web have made fighting online fraud akin to mounting an attack on bad weather. Stark's office receives about 400 complaints on a typical day. "With more investing in individual stocks than funds, more day trading, and more buying on impulse than sophisticated analysis, fraud has increased exponentially," says Lawrence Ponemon of PricewaterhouseCoopers, who heads a division that consults on fraud matters. Even organized crime is getting in on the action (see "The Shareholder From Hell," p72).

Since the NEI case, Stark's squad has been on a tear, helping the SEC break a series of high-profile cases. In August, the government nabbed Mark S. Jakob, 23, who allegedly issued a bogus press release stating that Emulex, a data storage firm in Costa Mesa, Calif., was under investigation by the SEC and that its CEO had resigned. In 16 minutes of trading, the company's shares plummeted, erasing $2.2 billion in market value. Jakob, who had both shorted the stock and bought it long, netted $241,000, according to the commission.

A few weeks later, the SEC settled a case with Jonathan Lebed, a 15-year-old New Jersey high school student. Without admitting guilt, Lebed agreed to cough up the $285,000 he made on 11 allegedly fraudulent trades between August 1999 and February 2000. And in September, Stark's team coordinated a sweep of 33 companies and investors who used the Web to "pump and dump" 70 penny stocks, running up their market value by $1.7 billion and reaping more than $10 million.

www.law.utoledo.edu/cybersecurities/

"I think they are doing a real good job," says Howard Friedman, a securities law professor at the University of Toledo and director of the Cybersecurities Law Institute there. "But, as is always the case with white-collar crime, it's always hard to keep a couple of steps ahead."

www.sec.gov/enforce/intrela.htm

Indeed, the SEC's Office of Internet Enforcement faces some tough challenges as it transitions from being a startup firing warning shots at online con artists to being a permanent, institutional fixture

Find this story online
Internet Keyword:
B2.0 New Untouchables
BUSINESS2.COM

DRAG.NET

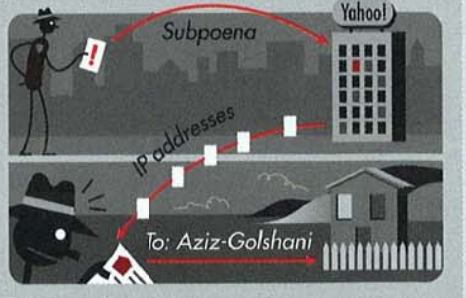
How the Feds caught two online stock swindlers.

1 Arash Aziz-Golshani and two friends drive up the stock price of NEI Webworld with hundreds of false messages on Yahoo! Finance and Raging Bull that said NEI was being bought. They pocket $363,991 in the scam. Their victims lose at least $400,000.

ALERT!

2 Cam Funkhouser of the National Association of Securities Dealers (NASD) tips off the SEC's top Net cop, John Reed Stark, about NEI's rocket rise and fall.

INTERNET TRACE



3 The SEC cybersleuths subpoena Yahoo! Finance and Raging Bull for the Internet Protocol addresses of the computers that sent the bogus merger messages. One IP address leeds the SEC to Aziz-Golshani's home computer.

Small cap and microcap
Companies deemed to be small caps usually have market capitalizations between $300 million and $5 billion while microcaps sport market values less than $300 million.

waging a perpetual cyberwar on stock fraud. So far it has adopted a strategy of making "message cases"—high-profile examples that alert investors to the different kinds of fraud they can fall victim to in the world of small cap and microcap stocks.

But now, some stock-fraud experts say the commission must go further and put more swindlers behind bars.

As a regulatory agency, the SEC does not have the authority to make arrests or prosecute offenders—those tasks fall to the Justice Department. As a result, the commission usually opts to settle civil lawsuits with fraudsters instead of referring every case for prosecution. Of the 209 total Net-related cases the SEC has handled, only 20 have resulted in criminal prosecutions. Michael Allison, CEO of Internet Crimes Group, a Princeton, N.J., private investigation firm, argues the SEC must become more aggressive to truly deter online stock fraud. "I commend the commission for the work they are doing," he says, "but unless their investigations lead to more criminal prosecutions, there will be this feeling that perpetrators are getting away with it."

Stark replies that given his unit's limited resources—just 15 investigators—it's difficult enough to gather sufficient evidence to file lawsuits against a handful of online grifters, let alone pursue hundreds of criminal cases in collaboration with the Justice Department. Says Marcy Ressler Harris, a lawyer who handles white-collar crime and securities cases for New York law firm Schulte Roth & Zabel: "It's impossible to catch everyone, so there is a great benefit to picking cases that warn the perpetrators and the public that this problem exists."

And there is another important consideration: Victimized investors want to recoup their losses, and that's much easier to achieve in civil proceedings, which move more quickly and necessitate meeting a lower burden of proof than do criminal cases. "Criminal prosecutions are not very good ways for investors to get their money back," says professor Friedman.

The Internet fraud unit also must walk the fine line between zealously pursuing online charlatans and respecting investors' privacy and First Amendment rights. No development better crystallizes this critical balance than the unit's move to upgrade the technological tools it employs to carry out its investigations. In late 1999, Congress appropriated $12.5 million for the office to beef up its fraud-fighting ability.

As a result, the SEC ordered a customized search engine for prowling message boards, Websites, and the hypertext-markup-language undergirdings of sites, for telltale signs of a scam. Examples of red flags: investment programs that promise incredible "high yield" returns of as much as 2,000 percent or the phrase *guaranteed returns.* ("There's no such thing," cracks Stark.) The search engine, which went live in the fall, is being built by SAIC, a San Diego firm that counts the Pentagon and the Department of Health and Human Services among its government customers.

Consumer and investor-advocacy groups say they worry that the search engine will help the government collect vast reams of public and private communications by honest, law-abiding investors. After all, though the Constitution does not permit individuals to use speech to swindle people, it does protect investors' right to excitedly trumpet the blessings of their holdings on message boards, email, or any other communications medium, even if their claims are inaccurate. "You have to recognize that in the zeal to catch these guys you may infringe on the rights on which this country was built," says Michael

Pyramid schemes
Many fraudsters have fused that old standby, the Ponzi or pyramid scheme, with online stock scams to create a potent hybrid. In 1999, for example, a Fort Worth, Texas, couple allegedly used a Website to sell $16.5 million worth of unregistered stock in their company, Cornerstone Prodigy Group, to 625 investors. In actuality, the funds of newly arrived investors became the profits paid to early investors.

4 Stark s team studies NEI trading data provided by the NASD and see that Aziz-Golshani and his two friends acquired 87% of NEI s stock in just three days.

5 Stark calls the FBI and federal prosecutors. They persuade an associate of Aziz-Golshani to wear a wire. He records incriminating conversations with Aziz-Golshani.

6 Aziz-Golshani and one of his two friends are arrested by the FBI. They both plead guilty to securities fraud. They are both awaiting sentencing.

Graphic by XPLANE | xplane.com ©2001

Shames, executive director of the Utility Consumers Action Network, an advocacy group in San Diego that uses its Website to alert consumers to possible pyramid schemes and other fraud.

Stark says the search engine will not be as invasive as some fear. While it will scan public message boards it will not poke into chat rooms, nor will it reach inside any individual investor's hard drive for data, he says. "This is not Carnivore," Stark says, referring to the controversial "sniffer" program being developed by the FBI. "We're just building our own Yahoo-like search engine that is customized to our needs. We will only use it to monitor what's publicly available."

Carnivore
To gather evidence on online criminals, the FBI is developing software that "sniffs" out email communications connected to lawbreakers. The FBI must obtain a court order before its agents can connect to an ISP's network and run Carnivore, and it says the program would not search beyond the specific criteria detailed in the order. But privacy advocates argue that the FBI would be privy to emails sent by honest citizens, a violation of a 1986 law that safeguards email.

Most of the technological tools the squad uses are in fact available to the public. In the NEI case, for example, the sleuths used a database of Internet protocol addresses on a site established by the nonprofit American Registry for Internet Numbers to locate the computer used to spread much of the fraudulent information about NEI. Still, as a regulatory agency the commission does have special powers. The NASD, for example, provides the SEC with trading data it does not share with ordinary investors.

www.arin.net

The Street Beat

From the outset, Stark set out to build a multidisciplinary squad of gumshoes (though almost all are lawyers). Matthew Moro, the unit's deputy chief, is a former assistant district attorney from Manhattan; David Gionfriddo, the office's No. 3 official, is a skilled legal writer; Bud Roth is a technology whiz who also speaks Japanese; and Irene Gutierrez is a money-laundering expert, formerly with the Justice Department. Other staff members specialize in areas ranging from the intricacies of securities law to litigation strategy. There's even Mark Wharton, on assignment from the U.K. equivalent of the SEC, to swap ideas and techniques with the Americans. "I wanted to set up a team of Untouchables," Stark says. To drive the point home, he has an original poster from the 1987 film *The Untouchables* on the wall of his office.

The rest of the crew: From left are Bill Hankins (*The NASD Expert*); Mark Vilardo (*The Professor*); Mike Monticciolo (*The Trading Expert*); Carolyn Gilheany (*The Sleuth*); David Gionfriddo (*The Wordsmith*); and Neil Miller (*The Intern*).

As for Stark, the 36-year-old alum of Duke University School of Law is an 11-year veteran of the SEC's enforcement division. Like any good hunter, Stark appreciates the cunning of his prey even as he tracks them down. For instance, showing off the unit's intranet on a computer in his office at SEC headquarters in Washington, Stark calls up an artifact from a 1999 case—a fabricated Bloomberg Website designed to boost a stock with false news. The G-man, who is fond of wearing cuff links bearing the SEC emblem, loves the fact that he can ride through this outlaw terrain with a badge pinned to his vest. "It's the finest job on the planet," he says.

The origins of the fraud unit go back to early 1995, when Stark realized how conducive the Net would be to perpetrating stock rip-offs. He set out to write a memo to his superiors detailing his ideas. It fattened into a 75-page white paper and concluded that the SEC should form a squad committed to waging a "counteroffensive" against online stock fraud. He handed it off to Gionfriddo, a friend from enforcement, who gave it a hard edit over a weekend. The final touch: Stark took the document to a Kinko's and had it copied and bound.

William McLucas, then the enforcement chief, and the commission itself were quick to accept Stark's case for a dedicated online stock fraud strategy, and the young lawyer was reassigned as special counsel for Internet projects. But, typical of federal agencies, Stark was not handed a sizeable budget (or even a raise) to carry out his new mission. Instead, he received five PCs and an AOL account. He also wasn't given a staff: Forced to rely on part-time contributions from other enforcement division staffers, Stark made only 19 cases between 1995 and 1997, when online trading started soaring.

By early 1998, a new enforcement chief, Richard Walker, had taken over, and he was concerned that Stark's fledgling initiative wasn't focused enough to meet the exponentially growing number of frauds. He was especially galled by how some fraudsters were openly bragging about how the SEC wasn't coming after them. "Touting doesn't mean anything to the SEC," boasted one, referring to the often fraudulent practice of hyping a stock. So, Walker met with Stark. "You're all over the place," the director said. "Your message isn't getting out."

Walker suggested that Stark adopt a stratagem right out of the Eliot Ness playbook—launch a raid.

They targeted touting first. Trading in hyped-up stock tips has long been a staple in the stock manipulator's kitbag. But the advent of online newsletters, message boards, and chat rooms were a touter's ultimate dream. It wasn't

Touting
A practice in which investment advisers, usually through Websites and online newsletters, recommend buying a security but fail to disclose that they are being compensated by the company being touted. Such an omission violates federal securities laws.

long before hundreds of newsletters and Websites were promising objective research and analysis on ready-to-rocket stocks—yet many were little more than nets designed to snag gullible prey.

The Net, however, also made dishonest touters easier to spot. "Remember," Stark says, "you're not trying to hide yourself when you commit this kind of fraud. You want people to contact you, and that leaves a resplendent evidentiary trail of spam, online newsletters, etc."

In October 1998, Stark's squad was ready. It launched its first sweep, filing 23 actions against 44 companies and individuals that allegedly touted more than 235 microcap companies unlawfully. The national press gave the raid a lot of play and Stark's office received more than 1,000 complaints a day for a couple of weeks afterward from concerned investors. By then Walker and the commission had seen fit to make Stark's initiative a full-fledged SEC unit, called the Office of Internet Enforcement. Stark received more funding (and his raise), more staff, and more technology. He reached out to other staffers in the enforcement division and formed the Cyberforce, a loosely knit group that monitors the Net for evidence in a particular case, or takes part in "surf days" when they troll for leads to possible fraud.

Rather than try and close every case it handled, Stark's unit took on the role of filter. It reviewed complaints, investigated enough to determine if there was a case, and then distributed the cases to the SEC's field offices across the country. It also served as a source of training and built a database of cases available to other SEC investigators, federal prosecutors, and the FBI. Before long, the unit had become the hub of a commission-wide effort to police the Net for

The SEC's Greatest Net Hits

Here's a sampling of the online stock frauds the Securities and Exchange Commission's Office of Internet Enforcement has helped expose:

Gold Spinners
In a variation of an old classic, David Abramson of New York allegedly claimed on his Website that his company possessed technology to transform a type of iron ore into gold. In exchange for an investment, Abramson allegedly promised investors returns of 800 percent to 2600 percent—all in gold. The SEC's lawsuit against Abramson is pending.

Football Fakers
Last September the SEC nailed Edgar A. Guilbeau of Houston and his firm, which claimed online to be a new NFL expansion franchise set to begin play in 2002. The firm offered stock in the team and dressed its site with the NFL logo and other trademarks. But the enterprise had no connection whatsoever with the franchise, and a judge froze its assets.

Tout Route
In the spring of 1999, Georgetown University law student Douglas Colt touted four stocks on his Website, driving up prices as much as 700 percent. He and his cohorts, including his mother, raked in more than $345,000. They settled with the SEC in March without admitting guilt.

Canned Scam
This case scores points for creativity: Lee Gahr, COO of a Nevada firm, allegedly claimed on Websites and in bogus unsolicited faxes that his company had invented an "environmentally friendly" self-cooling beverage can. Excited investors ran up the company's stock while Gahr allegedly sold it off, pocketing $277,136. Turns out Gahr's Arctic Can contained freon, a banned substance. The SEC's case is pending.

stock fraud. Stark's big idea in his 3-year-old memo, the formation of a dedicated squad of online enforcers, had become a reality.

Crime and punishment

Since then the unit has sought to take on more-complex market-manipulation cases, such as the NEI investigation. Increasingly, these cases involve a combination of cybersleuthing and old-fashioned shoe-leather techniques.

For example, at the same time that tech expert Roth and other members of the SEC unit were tracking down the PCs used to send the NEI spam, securities law specialists David Herman and Blair Vietmeyer were obtaining trading data that identified those who allegedly had sold blocks of NEI stock at big profits. The prime suspect was Arash Aziz-Golshani, then 23 and a UCLA graduate. When Stark learned of the investor losses involved—at least $400,000 total, with one investor alone dropping $127,661—he called Christopher Painter, an assistant U.S. attorney in Los Angeles who had prosecuted uber-hacker Kevin Mitnick in 1995. "I've got one you're going to love," Stark told him.

The FBI turned to a time-tested method for gathering evidence: An agent contacted an associate of Aziz-Golshani and persuaded him to wear a wire and record conversations about NEI with the suspect. It worked. Aziz-Golshani implicated himself in the fraud. They also obtained surveillance video from security cameras fixed around the biomedical library at UCLA that showed the suspects entering the facility on the days the bogus spams were posted. Last spring he and a co-defendant pleaded guilty to securities fraud charges and are now awaiting sentencing.

Given the apparent success the fraud squad is having in corralling online stock scams, it's tempting to ask Stark if he believes the SEC is actually winning the war. "That's tough to say," he says. "But on the Net I believe we are now perceived as a major police force."

While Stark has fulfilled Walker's wish that he deliver a message to investors to beware of online stock fraud, will they listen? Not likely, says Toledo professor Friedman. "It's real hard to figure out why people would not spend $300 on a television set without first reading up on it in *Consumer Reports* but will suddenly put $3,000 down on a stock they have barely read about," he says with a chuckle. "I'm not really sanguine that investors will begin doing more homework." Part of the reason, he says, is investors aren't cold-called during dinner with stock pitches that are easy to dismiss as bogus. Instead, eager investors "discover" data on their own, on message boards and Websites, an act that imbues the information with the credibility of an unearthed tip.

It's an interesting nuance, one that underscores how powerful the Net has been in subtly changing the attitudes of the public toward investing. Such attitudes will be difficult to change, if it's possible at all. So there is no doubt that fraudsters will continue to exploit the most gullible investor and that Stark and his new Untouchables will continue to watch stocks do funny things for years to come.

The trick will be to stay a couple steps ahead.■

EDWARD ROBINSON (EROBINSON@BUSINESS2.COM) IS A SENIOR WRITER IN THE NEW YORK OFFICE OF *BUSINESS 2.0*.