As Seen In Long Island BusinessNEWS Jul. 13-19, 2007

# Trade Secrets


By CLAUDE SOLNIK

It had all the elements of a Cold War espionage story by John Le Carré, except the secrets belonged to Coca-Cola, not the Central Intelligence Agency. This was a Cold War being fought between soda makers and soda spies.

The skulduggery started when Pepsi Cola executives last May received correspondence in an official Coca-Cola envelope. The contents were jaw-dropping.

The envelope contained a letter from someone nicknamed "Dirk," promising Pepsi sensitive information about Coca-Cola.

Dirk was Ibrahim Dimson, who with Joya Williams, a Coca Cola employee, devised a scheme to sell the Coke secrets. The two of them, plus another accomplice, asked Pepsi for $10,000. The tradeoff? Fourteen pages of highly-classified information.

The get-rich-quick plan died when Pepsi called the cops.

The story, if you recall, garnered national attention. But it wasn't unique, said John A. DeMaro, a partner at Ruskin Moscou Faltischek.

"I see an increase in trade secret-related litigation as well as criminal actions related to trade secrets," DeMaro said. "People are being more aggressive in keeping their confidential information secret."

Of course it's only in the biggest of situations that the Feds get involved.

### The real thing

The Feds might not be swarming on every deal, but prosecutors are aggressively pursuing criminal charges in cases of information theft from companies.

One key reason: They can.

The federal Economic Espionage Act of 1996 allows for up to 10 years in prison for thefts of commercial trade secrets.

Ethan A. Brecher, a partner at Liddle & Robinson, told The New York Law Journal that "private employers now have the ability to turn to the federal government for help in pursuing former employees for theft or attempted theft of their trade secrets."

The federal government has reportedly prosecuted nearly 40 trade secret theft cases under those provisions since 2000.

The prosecutors are certainly active in this state, where the Southern District of New York said in February that Ira Chilowitz, a former Morgan Stanley contractor, had plead guilty to stealing trade secrets, including client lists and formulas to calculate fees.

Another example: Edward R. Grande, of Bridgeport, Conn., was sentenced to 200 hours community service and five years probation for stealing trade secrets from Duracell Corp. Sentencing guidelines called for up to four years in jail.

The government has prosecuted those who have tried to sell MasterCard's secrets to Visa.

Closer to home, the Long Island Power Authority used all this to its advantage when it blocked a watchdog group's efforts to obtain copies of its power contracts with KeySpan. LIPA argued the contracts contained trade secrets.

Many of the cases are about employees taking lists, with companies claiming the lists are confidential. Employees, not surprisingly, disagree.

**Defining secrecy down**

The first question regarding the theft of secrets is whether information is actually secret. Joe Campolo, an attorney with a private practice in Smithtown said some people mistakenly believe many processes are proprietary.

> "People are being more aggressive in keeping their confidential information secret."

"Everybody thinks their software combined with their business products are protected trade secrets," Campolo said. "The analogy is, is it like the recipe for Coke or the process of Google? That's the issue. There's a threshold."

You can't argue something's a trade secret unless you try to prevent the public from knowing about it.

"You have to try and keep it secret," Campolo said.

The Economic Espionage Act indicates companies must seek to preserve secrecy with "reasonable measures."

Still, a secret doesn't even have to be a true secret for the government to prosecute. If an employee believes he stole a secret, that can be enough to trigger prosecution and conviction.

Brian Conneely, a partner at Rivkin Radler in Uniondale, said the speed with which information can become public online prompts companies to act fast.

"It's harder to claim something is a trade secret if it's published all over the Internet and is accessible by anybody employed by the company," Conneely said.

On the flip side, just because a company's information exists on the Internet doesn't mean it can't be protected. Campolo prevailed in a case where another company argued information wasn't secret because it was revealed in a patent application.

**Web of intrigue**

While people used to steal from file cabinets, the front lines in this corporate Cold War has shifted to computers. Hard drives make it easier to store and steal data.

**John A. DeMaro**

DeMaro said it's relatively easy to expropriate software source code, letting you crack and copy software.

That's what Chilowitz, a consultant for Morgan Stanley's information technology department, did, according to the U.S. AG's office.

Chilowitz was chased down by a computer crimes unit who followed footprints across cyber space.

"If somebody takes something deemed to be a trade secret, it's easier to track and trace through computers," Conneely said. "There is a trail."

Edward Grande, a battery cell development researcher at Bethel, Conn.-based Duracell, downloaded information about Duracell's AA batteries. He e-mailed the information to a home computer and sent the information to Duracell competitors, who sent the information to Duracell. Grande, for his efforts, ended up sentenced to five years probation.

In the meantime, the thieves keep on ticking.