

Reprinted from

AMERICAN BANKER

The Daily Financial Services Newspaper

Friday, July 14, 1995

Gumshoes Mine Data Bases To Ferret Out Fraud

By STEVEN MARJANOVIC

As a private investigator specializing in legal and financial cases, Jim Mintz stakes out the information superhighway, probing for data that individuals and corporations may not want to reveal to their bankers.

Mr. Mintz, president of James Mintz Group Inc., is often up against sharp-minded grifters who all too frequently dupe banks and others with exceptionally devious scams.

A seasoned investigator with 18 years' experience, he gathers information for litigation, due diligence, and other corporate and financial purposes.

He's racked up some impressive achievements, which include the hunt for Ivan Boesky's hidden assets in the Swiss Alps and the probe that sent a little old lady to jail for bilking a company for \$12 million.

But unlike the private eyes portrayed on television, Mr. Mintz, 40, does not carry a gun, nor does he engage in nerve-wracking car chases.

In fact, he rarely leaves his desk.

With the proliferation of such online data bases as Nexis/Lexis, CBD Infotek, Dialog, and Teledata, the days of gumshoe wear and tear are essentially over.

"It was kind of a musclebusiness, ex-cops really," recalls Mr. Mintz.

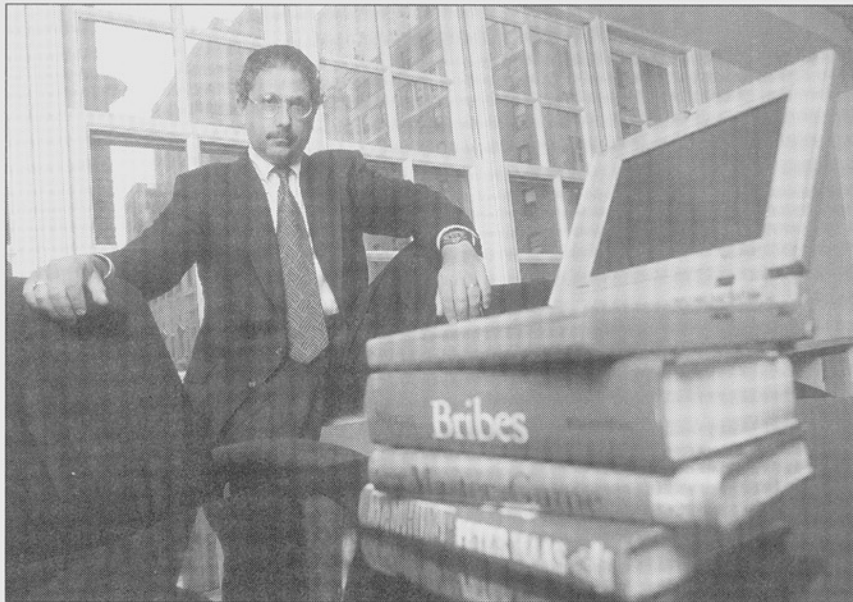
"You had to go out knocking on doors and having dogs bite you on the leg and stuff.

"But these data bases and other things have really fueled the change."

Employing six other private eyes in New York and Washington, the firm digs for dirt on credit applicants using a plethora of data bases, such as CBD Infotek, itself an amalgamation of data bases.

It offers address-change files and Social Security Administration death records, among other sources of information.

More obscure data bases include those that track yacht ownership, Nevada divorce records, and one that even one



JIM MINTZ heads a firm of private eyes who use brain, not brawn, to track down increasingly sophisticated fraudsters targeting financial institutions. Banks themselves are increasingly turning to on-line sources in due-diligence investigations.

Steven Hirsch

reveals which "private golf club a Japanese businessman belongs to."

"It's kind of difficult to count them all," Mr. Mintz admits.

However diverse the data bases are, they represent a tremendous resource when any one of his 24 bank customers wish to locate the assets a borrower might have squirreled away.

"We are strengthening a banker's hand in dealing with borrowers," Mr. Mintz says. "The further away from home a banker goes to do a deal, the less he's going to know about the people, and the less his gut instincts will help him."

He said he recently completed a successful investigation on behalf of a commercial bank.

The Federal Deposit Insurance Corp. had directed the bank to write off entirely a seven-figure loan, Mr. Mintz said. The bank hired the Mintz Group to find the assets.

Using information obtained through cross-referencing several more remote data bases, Mr. Mintz said, he was able to demonstrate that the borrowers

indeed possessed "significant dough."

"The bank held fast to its position and didn't write it off," Mr. Mintz said.

"They ultimately were able to settle it."

Many big banks, especially those with lots of foreign business, have become adept at fighting money-laundering schemes and other credit-related fraud.

But banks need to get even better at using all the resources available to detect scams, said Mike Anthony, a private investigator and executive vice president with Investigative Group Inc., New York.

"Banks have gotten much more sophisticated in terms of knowing what is available," he said, but "they still have a way to go."

Investigative Group, which Mr. Mintz helped found in 1984, is now a key competitor. Mr. Anthony headed First Chicago's due diligence operations before joining the firm.

Chemical Banking Corp., for instance, is among the institutions that frequently use on-line

data bases, including Mari, the acronym for Mortgage Asset Research Institute, and the International Chamber of Commerce, a London-based association that maintains a data base of attempted frauds.

"From our desks, my investigators can check motor vehicle records, Social Security records; we can check anything that's public," said Charles J. Bock Jr., Chemical's director of fraud prevention investigations.

Another senior banker, who requested anonymity, agreed that most major banks are proficient in obtaining all pertinent information for their due diligence operations, but, "as large banks become more sophisticated" in antifraud capabilities, so too do criminals, who are now targeting "smaller institutions."

"It's a trickle-down effect," the banker said.

Indeed, Robert H. Rasor, an assistant deputy director with the Secret Service's financial crimes division, said criminals are performing "due diligence in reverse."

"It's not so much what we

know; it's that the bad guys know how we do business," Mr. Rasor said.

"On a daily basis, they search or weaknesses in those business practices in which they can tweak themselves into."

He said criminals are able to entice banks with such seemingly attractive deals that banks may forego a thorough due diligence process for fear of losing the deal to a competitor.

"If you went back and did a restructured look at frauds that have occurred in the past, there's a good chance you'll find that someone came in with a high-dollar, short time-frame deal," Mr. Rasor said.

Indeed, *Business Week* this week reported on a scam that involved Guria, a privately owned company in the former Soviet Republic of Georgia.

Guria went for what seemed to be a good deal, the magazine said: 2,900 metric tons of sugar at \$265 a metric ton — well below the market price, which approaches \$400.

The magazine said that the shipment never arrived, but that according to the Secret Service a U.S.-based financier, William G. Moore, was able to cash in a letter of credit worth \$750,000.

Most U.S.-based banks will raise questions on such deals, Mr. Mintz said, but he pointed out that some crooked deals are not so obvious.

"Sometimes a bank's intelligence network can be strong in one area or in one industry, but not in another," he added.

Banks are approximately one third of Mr. Mintz's customer base, he said.

Some of those banks have strong investigative teams in-house, he said. He has worked with others of them to help demystify some of the data bases available.

Bankers need that kind of information for the snap judgments they have to make, he said.

"The crooks are smart," Mr. Mintz said.

"The people you are investigating are extremely international and have all sorts of tricks up their sleeves." □