

Checks & balances

Helping banks hold terrorists and drug kingpins to account

By **ROSS DALY**

Safe Banking Systems was showing off its scanning prowess to a potential bank client when the system did the equivalent of a bird dog's freeze and point.

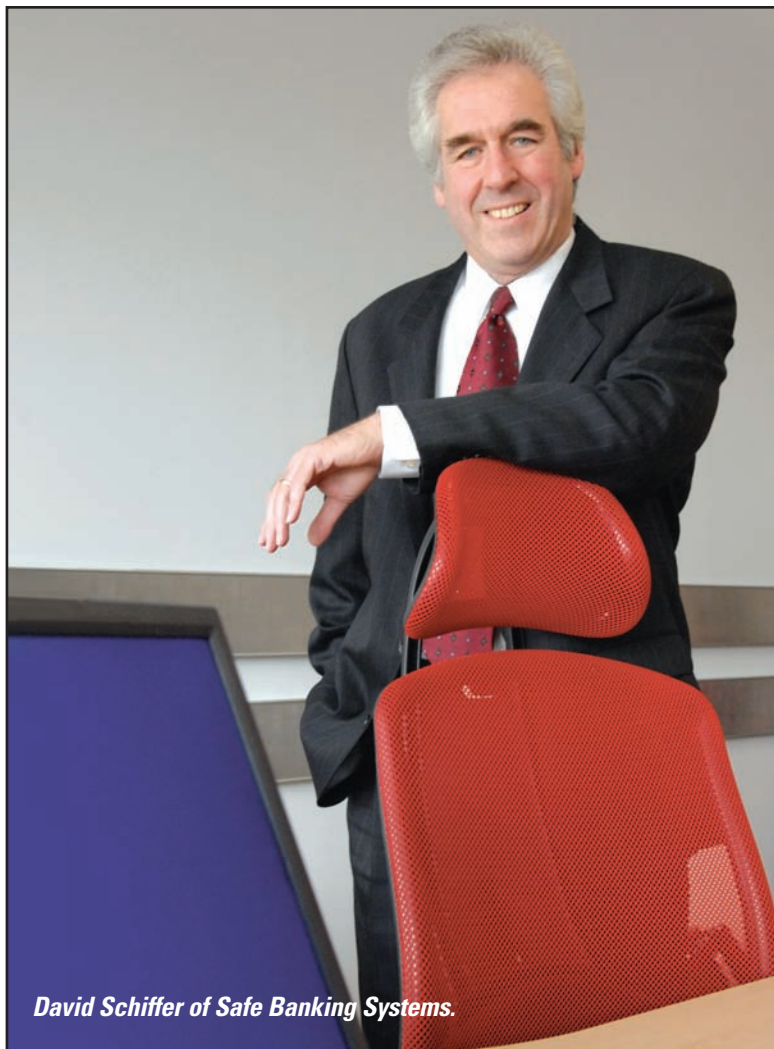
From among the thousands of account holders, up popped Olga Pinchouk, the wife of former Russian nuclear minister Yevgney Adamov. The couple was accused of diverting millions in American funding meant for nuclear plant safety to their own accounts, and Safe Banking had just found one. On a sales call.

You can't, as they say, buy that kind of marketing.

Operating out of an office with exposed brick walls and red modernist furniture – founder David Schiffer describes the space as “a Chelsea loft in Mineola” – Safe Banking helps banks and other financial institutions meet requirements for monitoring high-risk or illegal clients, including Colombian drug traffickers, corrupt foreign officials and international terrorists.

Among other unsavory characters Safe Banking searches have already turned up are an Al Qaeda financier with London and German addresses, a Taliban backer and a Jamaican narcotics kingpin.

“The fun is trying to design intuitive, easy-to-use tools in this



David Schiffer of Safe Banking Systems.

challenging area,” Schiffer said.

Virtual haystacks

Safe Banking hunts two levels of people. The first is a group named on what's called the “OFAC

list,” a compilation from the Office of Foreign Asset Control, a division of the U.S. Treasury Department. This list includes drug lords, terrorist organizations and international baddies from

such places as North Korea and Syria.

U.S. banks are prohibited from having relations with such people. When discovered on a customer list, the bank must terminate relations and freeze any pending transactions. This is the straightforward side of the business.

The second category presents more complexity; it's broader and less defined. This is a group known as "politically exposed persons," or PEPs in the acronym-laden world of financial security. These people may pose a risk, but not one so clear-cut as the threat posed by the OFAC list. PEPs include senior foreign political figures, including heads of state, cabinet members, ambassadors, judges, party officials and military leaders, as well as their family members and close associates.

"They're allowed to have bank accounts, but they're not allowed to use them for corruption or terrorist financing," Schiffer said.

Tracking this ever-changing and much larger group is at the heart of Safe Banking's expertise. Government doesn't supply a list

and there isn't even an international agreement on what constitutes a PEP. Instead, those monitoring financial transactions rely on firms that supply lists, and it can be a "crazy, difficult burden," according to Schiffer.

"The government is making financial institutions cops," he said.

Safe Banking uses World Check, a British firm that produces a list of several hundred thousand names, updated daily. World Check assembles its list by monitoring the Internet and media sources worldwide. Safe Banking then plugs the PEP list into systems from Fircosoft, a French company that develops software for name matching that uses what's called "fuzzy logic" – basically, a match doesn't have to be exact.

"It's a big problem when a bank has 10 million accounts and you have a list with hundreds of thousand of names, and different cultural naming conventions, aliases and transliterations," Schiffer said.

Schiffer, a Bronx native and

one of the first graduates class in computer science at Stony Brook University – the Class of '72 – launched Safe Banking in 1998 after years in the computer and international banking trades. Today, the firm employs nine full-time employees and five part-time, although Schiffer hopes to expand to 12 full-timers this year.

The staffer with the longest ties to Schiffer: His son Mark, the firm's chief of research and development. He joined the firm about five years ago after attending Wharton Business School and writing and directing a well-received independent film, "Strong Island Boys." Mark Schiffer has developed a number of the applications that Safe Banking employs.

Small player, big world

The system Safe Banking uses offers each client a customized list based on a pre-determined level of risk. That can range from the highest risk account-holders to those who would merely cause embarrassment if the relationship were made public.

If politically exposed persons are detected, companies can monitor their financial activity to ensure it doesn't put the financial institution at risk.

Potential customers send over 5,000 to 10,000 sample accounts and Safe Banking runs a test and issues a report, as happened in the case of the wife of the former Russian nuclear minister.

"We get a lot of our business through proof-of-concept," Schiffer said.

The samples, like the real-world product, produce alerts and allow compliance officers to determine if their account-holder is, in fact, the person on a given watch list. The visual displays show locations the person has visited or lived in, aliases, ties to companies and individuals, circles of friends and relevant news accounts.

"There is complex stuff behind it," Schiffer said, "but we try to make it easy to use."

Smart cards, smart crooks

Safe Banking is not the only private firm keeping a watchful eye on bank transactions. Melville-based Epoch Data covers another corner of the anti-money-laundering field, offering financial institutions real-time transaction monitoring to comply with anti-money-laundering regulations and to help prevent fraud.

Epoch's system gathers data from ATMs, bank tellers and other sources, processing up to a million transactions per second, according to Paul Silverstein, the company's executive vice president. When unusual or suspicious activity is detected, alerts sound for closer monitoring; transactions

such as wire transfers can then be put on hold.

One focus of Epoch's work is detecting fraud connected to what the industry calls "stored value cards." You know them better as gift cards. Criminals steal credit cards, then use them to purchase gift cards, which can be used to purchase goods that are then returned for cash. The cards are also routinely "e-fenced" over the Internet.

Even if the credit cards theft is detected, tracking which gift cards were purchased illegally is complicated.

"It extends the life of the crime," Silverstein said. "It's a race against time."

– **ROSS DALY**