

Originally published in The Globe and Mail, April 16, 2008

Anti-laundering software casts wide net to catch big fish

Powerful computers and constantly tweaked software plow through mountains of customer data looking for suspicious activities – such as a state governor transferring large amounts of cash

IAN HARVEY Special to The Globe and Mail Published on Wednesday, Apr. 16, 2008
11:55PM EDT Last updated on Monday, Mar. 30, 2009 3:29PM EDT

Poor Eliot Spitzer. The former governor of New York resigned in disgrace last month amid allegations he hired a high-priced call girl. In a matter of days, Mr. Spitzer went from potential presidential candidate to — in the tech world, at least — the poster boy for software usually used to snare fraudsters, money launderers and terrorists.

With an estimated \$500-billion to \$1.5-trillion (U.S.) a year laundered globally — the bulk of it from drugs and organized crime — banks use anti-laundering software to plow through mountains of customer data looking for suspicious activities, says Wes Gill, enterprise risk manager for SAS Canada, which makes an anti-laundering software product.

The software looks for subtle patterns that indicate odd activity, and when a transaction is flagged, a human evaluates the findings. More often than not, the anomaly is explained and dismissed. For example, someone whose banking consists of bi-weekly deposits may suddenly show an influx of \$15,000 that turns out to be profit from the sale of a car.

But when investigators do find something — like chunks of money transferred from the account of a state governor into the account of a shell corporation — they flag the information and forward it to the authorities. In the United States, the U.S. Treasury's Financial Crimes Enforcement Network looks at almost five million suspicious activity reports a year. In this country, The Financial Transactions and Reports Analysis Centre of Canada in 2007 investigated 193 cases involving close to \$10-billion in financial transactions.

"There are two things the banks want," Mr. Gill says. "One: to flag money laundering ... and two, to detect fraud. But there are literally millions of transactions a day. That's why the technology is so critical."

So it wasn't dumb luck that Mr. Spitzer's bank uncovered the abnormal activity. Powerful computers running various vendors' anti-fraud software analyze almost every transaction processed — as many as 50 million a day. But what tweaked the software in Mr. Spitzer's case was not money moving from point A to point B. In fact it was the former governor's efforts in trying to conceal the transactions that triggered the alert, authorities say.

By law in Canada and the U.S., banks are obligated to report cash transactions of more than \$10,000. According to U.S. federal officials, Mr. Spitzer's transactions were flagged because it appeared as though he was trying to evade notice by moving several smaller amounts, which is known as "structuring." In Mr. Spitzer's case, three cash transactions amounting to more than \$10,000 within a relatively short time frame set off alarms.

"Spitzer is a perfect example of how people are constantly trying to manipulate the test so they can come in under the radar," says John Wall, chief technology officer of Symcor, the company that processes cheques for Canadian banks.

With literally hundreds of millions in credit and debit card transactions, transfers of stocks and bonds and electronic and cash exchanges, the trick for banks is to find a balance between generating too many flags and too few. And since Sept. 11, 2001, banks have come under even more pressure to report any kind of questionable activity that might relate to terrorist financing.

The challenge for the software, Mr. Gill says, is to prioritize those transactions that are most suspicious, and at the same time reduce the number of false-positives — transactions that are flagged, but aren't suspicious. In order to do so, the software runs on a set of rules that are always being tweaked. Account holders are also rated by risk factors in order to generate behavioural baselines, so a nurse or mechanic would likely not get the same scrutiny as, say, a public official.

"We uncover 98 per cent of cases that we come across [using] the technology," says Daniel Tobok, president and CEO of Digital Wyzdom, a financial forensic investigation firm.

The fact that almost all transactions are now electronic transactions is a two-edged sword, notes René Hamel, a former RCMP officer who is the director of forensic technology services with KPMG in Dublin. The massive volume of data and the anonymity of cyberspace imparts a secure feeling on those manipulating the system, but that's offset by the increasing power of the technology and software, he says.

Once a transaction or series of transactions are flagged, investigators can start looking at other points of data around those transactions.

"You want to add to the story," he says. "So if the transactions were on a Sunday, you'd start looking at the building data — who was working on a Sunday, for example, whether those people or that person often worked Sundays. You'd look at all their e-mail, BlackBerry and other network activity."

Of course, he says, sometimes there are innocent explanations, which is why there has to be a human element. And sometimes there aren't, he says, in which case the technology becomes an indispensable investigative tool.

BY THE NUMBERS

- 193 — Number of cases Canada's financial intelligence unit investigated in 2007
- 152 — Number of cases for suspected money laundering
- 33 — Number of cases for suspected terrorist activity financing and/or other threats to the security of Canada
- 8 — Number of cases that involved both suspected money laundering and suspected terrorist activity financing and/or threats to the security of Canada
- 458 — Average number of transactions examined in each case
- \$9.8-billion — Total value of transactions

Source: Financial Transactions and Reports Analysis Centre of Canada