

Please note that this material is copyright protected. It is illegal to display or reproduce this article without permission for any commercial purpose, including use as marketing or public relations literature. To obtain reprints of this article for authorized use, please call a sales representative at (818) 461-9700 or visit <http://www.ectnews.com/about/reprints/>.

Big Blue Dons Big Data Gloves to Fight Fraud



By Richard Adhikari
E-Commerce Times
03/21/14 6:37 AM PT

[A A Text Size](#)
[Back to Online Version](#)
[E-Mail Article](#)

IBM has taken on the big challenge of fighting financial crime by creating a coherent analytics system capable of sussing out non-obvious relationships in the masses of Big Data enterprises collect. The problem for companies like Target has been too much information. IBM aims to determine where likely trouble spots are early enough for them to take meaningful action.

▼ advertisement

Webinar: The New PCI 3.0 Standard

Learn the steps to take to get your company ready for PCI DSS 3.0 changes coming January 2015. We cover all of the details you need to know as we head to the deadline to complete and pass your PCI DSS 3.0 audit. [View the PCI Webinar Series Now.](#)

IBM on Thursday launched a set of software and consulting services to help fight fraud and financial crime.

The so-called smarter counterfraud initiative draws from more than 500 fraud consulting experts, 290 fraud-related research patents, and the US\$24 billion IBM has invested in its Big Data and analytics software and services capabilities over the past nine years.

The software lets organizations aggregate data across multiple internal and external sources, including mobile, social and online, and apply analytics that continuously monitor the data for indicators of fraud. The analytics understand non-obvious relationships and co-occurrences between entities, among other things, leveraging IBM's work in artificial intelligence.

"The problem we're addressing is in many ways looked at from singular dimensions within the enterprise," Bob Griffin, vice president, IBM Counter Fraud Solutions, told the E-Commerce Times.

"People look, for example, at cyber as one area and transactional issues as another, and identity as another -- and historically, many of those silos didn't communicate with others," Griffin explained. "Sometimes when you see events in one silo they may be misrepresentations that distract you while the real attack comes from elsewhere."

The distributed denial of service, or DDoS, attacks launched against banks are a good example. IT focused on battling the DDoS attacks while the fraud was "coming in through the back door and picking your pocket," Griffin said.

Big Blue's Offering

IBM's Counter Fraud Management software includes analytics that understand non-obvious relationships, visualization technology to identify larger patterns of fraud, and machine learning to help prevent the recurrence of attacks.

"Everybody collects information in the enterprise space," Mike Jude, a program manager at [Frost & Sullivan](#), told the E-Commerce Times. "The secret sauce IBM is offering is the analytics."

IBM also launched IBM Red Cell, a new counterfraud intelligence unit, on Thursday.

IBM's counterfraud services include evaluating a client's counterfraud capabilities and providing rapid prototyping; designing organizational constructs, operational governance and technology architecture to help detect fraud and respond and investigate exposures; and implementation of strategies and technologies to create and run customized counterfraud programs.

Big Blue also will offer a portfolio of customizable assets that use analytics to discover fraud, waste, abuse and errors in data-intensive industries and functions, focusing on medical, insurance claim, public tax and occupational fraud. These will be available in the cloud, enabled by IBM SoftLayer.

Everything Old Is New Again

The idea of using Big Data analytics has been around for awhile.

The [Aberdeen Group](#) discussed this in a 2012 [report](#).

Hortonworks and Pactera held a [webinar](#) on how Big Data is revolutionizing fraud detection in financial services last fall.

The [United States Postal Service](#) has been using Big Data to fight fraud for years, relying on an architecture it began building in 2006 that processes data on about 530 million pieces of mail daily.

Making Things Practical

As of 2011, the typical organization [was losing](#) 5 percent of its revenue to fraud annually, according to the Association of Certified Fraud Examiners.

By 2012, global credit, debit and prepaid card fraud [losses totaled](#) nearly \$11.3 billion, [according to the Nilson Report](#).

The problem is not that we don't have enough data, but that we have too much and can't focus on the critical information in a timely fashion, Frank Dickson, industry principal for network security at Frost & Sullivan, told the E-Commerce Times.

"Target was alerted there was a problem two weeks before they were breached but they didn't do anything because they had too much information," Dickson pointed out. "We don't need more alerts, we need to be actionable."

Big Data analytics makes information actionable, Dickson said. "That's what's going to distinguish the successful players in the market." **101**

Richard Adhikari has written about high-tech for leading industry publications since the 1990s and wonders where it's all leading to. Will implanted RFID chips in humans be the Mark of the Beast? Will nanotech solve our coming food crisis? Does Sturgeon's Law still hold true? You can connect with Richard on [Google+](#).

 [Get Permission to License or Reproduce this Article](#)

 [Print Version](#)  [E-Mail Article](#)  [Reprints](#)  [More by Richard Adhikari](#)