Forbes

September 22, 2014

How to Use Big Data To Fight Financial Fraud

By: Sarah Diamond, IBM

Commerce has gone digital and so have the fraudsters. Big data and analytics are our greatest weapon against them.

Although the digital era has improved our lives in many wonderful ways, there is another side: fraud is flourishing at an alarming rate. It's impossible to measure the precise cost, but we know it's not trivial. Consider:

Businesses lose an estimated $3.5 billion annually to fraud and financial crime, according to the Association of Certified Fraud Examiners.

Fraud losses are estimated to total $80 billion per year in the health care sector alone, the Coalition Against Insurance Fraud says.

Non-health-related insurance fraud is believed to top $40 billion annually, according to the FBI.

Identity theft of credit cards in the U.S. added up to almost $25 billion in 2012, the federal Bureau of Justice Statistics says.

It's a crippling problem for large corporations, particularly for data-intensive industries, such as Financial Services, Government and Healthcare, because vast pools of data inadvertently mask fraud. Roughly five percent of an average organization's revenue is estimated to be lost to fraud.

In many cases, the short-term financial loss is negligible compared to the long-term loss of valued customers who are no longer comfortable buying from merchants whose networks have been hacked. In the frenzied rush to move business online, security has sometimes been compromised. The same things that make digital commerce attractive to businesses — efficiency, speed, global accessibility — make it equally attractive to criminals.

We can't eradicate fraud altogether, but there is much more we can do to fight it. The first step is to better understand and predict where fraud might occur. Data and analytics is the best — if not the only — way to do this.

And your company can house the information in a cloud.

Once primarily used to run back-end infrastructures for a handful of large corporations, now any company with a digital sales platform probably has at least a part of its business in the cloud. In terms of fraud prevention, the cloud allows organizations to consolidate and analyze sales data from disparate sources in one place. Transactions generated over a mobile app, in a store or in an office, can all be accessed and analyzed over the cloud in nearly real-time.

Many companies already use analytics to identify normal sales patterns. They know, for example, how each product sells every day of the week, in which zip codes and at what prices. Once they know what normal sales look like, they can sniff out aberrations almost immediately — before they become multi-million-dollar security breaches.

We can also use analytics to look for typical patterns of behavior. If a specific customer usually logs on to a commerce site over her phone and spends no more than $140, the merchant and the customer can immediately be alerted to someone logged on to the site under her account from a dial-up connection and spending upwards of $600.

Organizations that are serious about mitigating fraud also need to look internally and make changes from the top down. Again, data and analytics can help public and private enterprises determine which positions have the highest average losses, and which employees may have the most incentive and opportunity to commit fraud. If a specific regional office suffers higher fraud rates than others, security teams can investigate former employees in the area, test for network vulnerabilities, and see if there are unique processes in place that are failing to catch or prevent fraud.