CLABBY ANALYTICS

Research Report

IBM's Smarter Counter Fraud Initiative: A Comprehensive, Unique and Aggressive Approach to Real-time Fraud Prevention

Executive Summary

By combining and integrating numerous IBM software products (security, data management, entity/predictive/behavioral/context/content/geospatial analytics, social network analysis, forensic analysis, case and content management, middleware and more) IBM has been able to build a comprehensive, integrated fraud prevention environment designed to detect, respond to, investigate and discover fraud activities in real-time. Further, IBM has augmented this environment (known as IBM Counter Fraud Management) with additional security and deployment services.

> ***From our perspective, no other security/fraud vendor has even come close to IBM in terms of counter fraud product breadth and depth – nor in related security services. The way we see it, IBM's competitors offer – for the most part – point product, custom or appliance solutions, whereas IBM's new offering is a complete, integrated anti-fraud architecture.***

In this *Research Report*, *Clabby Analytics* takes a closer look at IBM's new Counter Fraud Management environment. We consider the state of the fraud market today; we discuss the need for fraud prevention and advanced counter fraud management; and we describe how IBM's Counter Fraud Management framework works. We also describe why we believe that IBM's new counter-fraud environment is unique as compared with other anti-fraud offerings from other vendors. Further, based-upon our attendance of IBM's Counter Fraud Management Initiative announcement in NYC, we share some customer insights related to fraud management. Not to be overlooked, we also describe IBM activities in security intelligence – including the formation of IBM's Red Cell organization which compliments IBM's X-Force security intelligence activities. Finally, we conclude with the following finding: "enterprises that are looking to stem losses due to fraud need to take a holistic approach to fraud prevention and management – and IBM, with its Counter Fraud Management environment has architected such a holistic offering".

The Market: Huge Losses, and the Bad Guys Are Winning

Fraud is one of the world's largest businesses. "Bad guy" individuals and organized crime organizations defraud enterprises and individuals of almost $3.5 trillion in revenue and saving each year – and this number is growing (it currently represents about 5% of the world's total gross national product). These bad guys are well financed; they are not regulated; they are innovative and creative – and they only have to get one intrusion sequence right in order to defraud others (whereas enterprises and individuals cannot afford a single intrusion). Cyber fraud has reached such an alarming rate that U.S. Army General Keith B. Alexander (the director of the National Security Agency [NSA] and chief at the Central Security Service [CSS]) has

called cybercrime: "the greatest transfer of wealth in history" (see this article for more of Alexander's assessment of the worldwide fraud situation).

Given this backdrop, it is clear that the "good guys" need to get a lot better at fraud prevention and at counter fraud management. But the biggest obstacle that enterprises face in combating fraud may be self-created: too many organizations are segmented and siloed – so internal departments have been known to attack fraud individually according to their chartered mandate – while not working together with other internal organizations to conquer fraud holistically. Further, some enterprises successfully attack fraud but are loathe to share their experiences – failing to collaborate with other enterprises that are facing the same risks. Using a collaborative team approach puts more people into the pool of fraud problem solvers – helping to put more and more fraudsters behind bars – which is a good thing for *all* enterprises.

Before IBM's announcement of its Smarter Counter Fraud Initiative, we would have argued that software integration was a major obstacle when it came to preventing and countering fraud. Siloed departmental behaviors and lack of collaboration remain organizational issues – but, with IBM's Smarter Counter Fraud Management environment, IBM has found a way to mitigate security and fraud management integration problems. In fact, we believe that IBM's integrated Smarter Counter Fraud software environment may also help overcome organizational issues as fraud managers will now have access to the same data and the same tools that can be used collaboratively to help defeat intruders.

IBM's Smarter Counter Fraud Initiative: A Holistic Approach to Prevention and Counter Fraud
A very close look at IBM's Smarter Counter Fraud Management solution shows that it is comprised largely of security tools, analytics tools and risk management tools.

For the past three years *Clabby Analytics* has been pointing out that IBM is building a major competitive advantage in the field of analytics. We have seen huge investments in analytics research and development – and we've seen huge investments in analytics-related acquisitions (including the acquisition of SPSS, StoredIQ, Star Analytics, TeaLeaf Technology, The Now Factory, and others). We have seen no other major competitor invest as heavily in analytics as IBM.

We have not, however, been reporting with regularity on IBM's rapidly expanding security and risk management portfolios. From a security perspective, since 2010 IBM has acquired the National Interest Security Company, Q1 Labs, Trusteer and more. These acquisitions, when combined with IBM's internally developed security portfolio, help prevent intrusion by providing a deep and comprehensive security environment that can be used to secure systems and authenticate users; establish security policies and procedures; and implement rules and automate security activities. In risk management, IBM's own risk management tools have been complimented by the acquisitions of Open Pagesand Algorithmics.

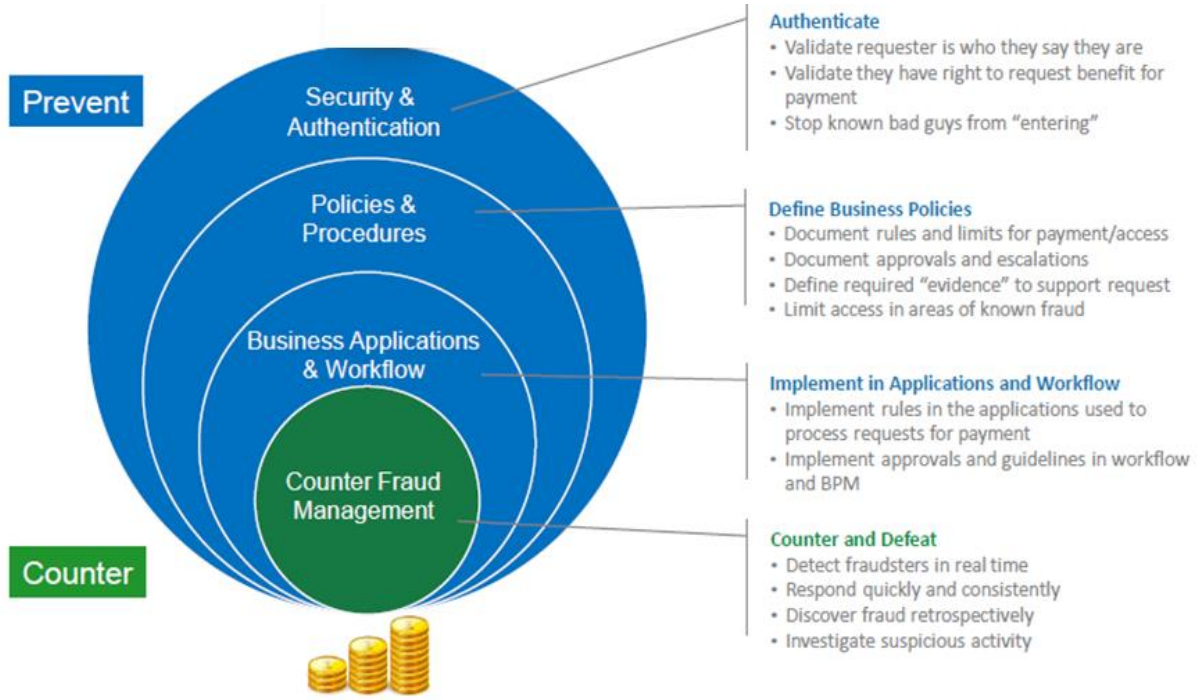
For a more complete list of IBM analytics, risk and security acquisitions, see this Wikipedia listing.

With a vast amount of internal intellectual capital – and with acquired intellectual capital – IBM is able to pick-and-choose the software elements that it needs across its broad portfolio to construct new, integrated solutions. As we will show later, this is exactly what IBM has done as it architected its Smart Counter Fraud solutions.

The Big Picture

IBM's Counter Fraud Management environment now extends IBM's security/risk management portfolio by adding a deep counter fraud environment that works in tandem with other IBM security products (see Figure 1 for a big picture description of how IBM security and counter fraud environments work together to reduce and/or eliminate security/fraud breaches).

Figure 1 – The Big Picture: Security and Fraud Prevention Working in Tandem



Source: IBM Corporation – March, 2014

With the addition of an integrated counter fraud management environment to its security and risk management portfolios, IBM has created a holistic intrusion prevention and counter fraud management environment that is unrivaled by any competitor.

A Closer Look at IBM's Smarter Fraud Management Solution

How does IBM"s Smarter Fraud Management framework work? Let's start with what enterprises are managing fraud activities today. Fraud management activities today are generally structured to prevent fraud (fraud defense), as well as to stop fraud from occurring (counter fraud). Fraud defense activities include cybercrime protection, as well as the implementation of various controls (such as setting thresholds), policies and processes. Counter fraud activities include *detecting* fraud, *responding* to fraud by stopping a transaction or letting it proceed, *investigating* suspicious activity – and, in some cases *performing discovery* (taking a look at past behaviors to look for retrospective linkages between events).

To conduct prevent fraud and to counter fraud activities humans need to evaluate a wide variety of situations (claims, out of character activities, etc.) looking for anomalous behaviors. And to do this more effectively, enterprises invest in a variety of tools. For instance, in fraud defense tools are used to protect against malware, to determine risk, and to set up policies and procedures. In fraud management, various tools are used to:

- Perform multi-layered analytics using business rules can be used to perform predictive, entity, context and behavioral analytics – all of which streamline fraud ***detection***;
- To speed ***response*** time (decision management tools);
- To help ***investigate*** potential fraud (forensic and case management tools including social network, geo-spatial and context management tools); and,
- To ***report*** – including tools that can be used to model operational risk, examine fraud exposure – and to create evidence that can be used to prosecute wrong-doers.

IBM's Smarter Counter Fraud software portfolio is comprised of a wealth of fraud management and fraud defense – all of which work together in an integrated fashion to help prevent fraud:

- The fraud management portfolio consists of a variety of product that help:
    - Detect fraud (SPSS, Identity Insights, Context Analytics – and can use InfoSphere Streams and InfoSphere BigInsights to organize data for analysis);
    - Respond to fraud attempts such as IBM Decision Management;
    - Investigate fraud attempts (i2, Advances Case Manager, and Content Analytics – and IBM's Tealeaf offering); and,
    - Discover instances of fraud (SPSS, Content Analytics, Cognos BI, Counter Fraud Discovery – and also GBS Services Assets such as FAMS).

- The fraud defense portfolio includes products that help:
    - Detect fraud (Trusteer Pinpoint Malware Detection and Trusteer Pinpoint ATO Detection;
    - Respond to fraud attempts such Trusteer Rapport and Trusteer Mobile Risk Engine;
    - Investigate fraud attempts (such as Curam and IBM Security Access Manager); and,
    - Discover instances of fraud (including OpenPages and InfoSphere Guardium Data Security).

It is important to note that fraud management is largely a Big Data analytics activity. What this means is that the above-listed analytics tools will need to comb through large data sets looking for anomalous behavior. This necessitates that enterprises take a disciplined approach toward organizing and managing the data that they intend to use for fraud detection purposes. IBM's Smarter Counter Fraud software is an extensive set of tools that can be used to analyze fraud behaviors – but the results are only as good as the database that is being analyzed. So enterprises that want to build highly effective fraud management environments need to start by cleansing and organizing their databases.

The Competitive Scenario

A quick Google search on fraud management and fraud detection will yield numerous product offerings from various vendors that are involved in various aspects of fraud management such as detection, investigation, and reporting. Some of these vendors include SAS, Experian, Detica, Lexis/Nexis, Symantec, Actimize, Volance, CSC (with Fraud Analytics), Netcraft, Entrust, Neustar, Socure, Wells Fargo and FICO. Several of these vendors offer point products designed to deliver specific fraud solutions, others offer base products and customization services – and still others offer appliance-oriented (black box) approaches. SAS, a leading maker of business analytics software offers analytics solutions that can be customized to meet enterprise analytics needs. Detica's offering is more of a blackbox appliance approach. While FICO and Actimize offer several fraud management solutions (for instance FICO provides analytics and decision making services; while Actimize provides financial crime prevention, compliance/risk management products/services for the financial services industry). (Note: IBM's Smart Counter Fraud Management environment has been designed to serve multiple industries including financial markets, healthcare organizations, governments and insurance companies. IBM has created special "patterns" with industry-oriented functionality designed to help managers, administrators and investigators solve problems specific to their particular industries).

From our perspective, the primary differentiators between IBM's Smarter Counter Fraud Management framework and the offerings of its competitors is the depth and breadth of its product offerings. IBM is one of the largest database companies in the world – so it owns and controls fast databases and related data management environments. IBM servers process a huge number of transactions daily – and have a strong reputation for trustworthy, secure computing. IBM offers the middleware linkage that enables programs and data to work together seamlessly. And, as a result of numerous business analytics, risk and security acquisitions – IBM now has a broad fraud prevention and management portfolio. No other vendor in the list above owns all of these components – and, accordingly, providing integrated solutions means that these vendors have to work together with 3rd parties that may or may not have the same priorities as these fraud prevention/management vendors. IBM's strength, depth, and breadth of systems/systems software/middleware/operating environments/-management software and fraud/security solutions positions IBM to do a better job at integration than its competitors – and positions IBM more clearly as the builder of a complete end-to-end architecture as compared with point or appliance approaches.

Customer Perspectives

Clabby Analytics attended the announcement event for IBM's Smarter Counter Fraud initiative. At this event numerous customers shared their perspectives on fraud – and their opinions on the need for more integrated fraud management offerings. The list of customers who presented their opinions on stage included SunTrust Bank, the office of the medical inspector for New York State, Westfield Insurance, Bank of America, and the New York State Tax Division. These customers spoke on a number of topics – but the following insights resonated most with us:

1. One of the biggest issues faced by customers is related to ***data*** (more specifically, getting their databases in order). These customers need production data that has been filtered and formatted in such a manner that it can be more easily analyzed by analytics tools.
2. ***Organizational behavior*** is a major issue. Customer after customer described how various departments within their organizations have responsibilities that may overlap with several department charters; how different databases are being used; how different

tools are being used, and how conflicts regularly arise. To remedy this situation (intimated one customer) – strong executive management needs to get involved to set clear goals and responsibilities. According to some attendees, siloed behavior should not be tolerated – it is inefficient and counter-productive.

3. ***Collaboration*** was also identified as an issue. Internal collaboration issues were described in point #2 – but external collaboration was also raised as an issue. Customers expressed a desire to marshal forces from a wide number of forces to help combat today's and tomorrow's fraud attacks.
4. ***Resource utilization*** was also raised as an issue. Fraud management practitioners expressed the need for their own enterprises to assign the right resources to the projects *based on the biggest return-on-investment*. These practitioners called for more tools and broader capabilities for fraud analysts – especially for more predictive analytics modeling tools. And, finally,
5. ***Skills*** were identified as an issue. *Clabby Analytics* has written several reports on the general skills shortage that affects the IT industry (in areas such as Windows and Linux management, Java programming, and so on). In analytics, we have pointed out that there is a constant need for more and more data scientists (and we have noted that IBM is funding analytics training programs at several colleges and universities including IBM's analytics solutions center at Purdue University in Columbus, Ohio – as well as building "centers of excellence" around the globe). And we have also pointed out that IBM is spending millions and millions of dollars simplifying its analytics products such that "the common man" can use business analytics tools without having to learn special programming and query skills. Finally, note that IBM has hired thousands of data scientists to pre-build query solutions – so that, according to one IBM executive, "our customers don't have to invest heavily in finding staff to query databases".

Intelligence Research

As we mentioned in the *Executive Summary*, IBM also conducts security intelligence activities to help identify threats and to help IBM customers better prepare for security threats. To this end, two organizations (IBM's X-Force and Red Cell organizations) work in tandem to help customers better understand the threat landscape and take appropriate actions to counter threats and fraud:

- IBM's *X-Force* is an organization that monitors and evaluates the rapidly-changing security landscape (IBM's Trusteer endpoint intelligence is used heavily by this organization). X-Force researches new attack techniques and develops counter protections against those techniques. And X-Force helps drive inter-/intra-enterprise collaboration. Samples of IBM X-Force reports can be found here.

- IBM's *Red Cell* organization is essentially a security task force that makes use of X-Force reports and other data sources as it monitors emerging trends in financial crime across industries and around the world. Red Cell specialists have deep experience in fraud management and provide cutting-edge thought leadership to counter and prevent fraud.

Both organizations create opportunities for intelligence sharing amidst public and private companies, and work in tandem to continuously research trends, develop strategies, and deliver enhancements to the software and services R&D team.

Related Professional Services Offerings

IBM's Global Services organization draws on the of more than 500 fraud consulting experts, 290 fraud-related research patents and the intellectual capital derived from over $24 billion invested in IBM's Big Data and Analytics software to help public and private organizations prevent, identify and investigate fraudulent activities. IBM's counter fraud service offerings include industry-aligned services that combine IBM's consulting, software and technology expertise to help clients improve their counter fraud programs. Some of these services include acceleration programs that help organizations move more aggressively in fraud management; operational models (that can help organizations overcome the organizational behavior/silo problems described earlier); and services that can help organizations more effectively manage growth (scale) to deal with increasing demands for more fraud management protection.

The Future: Fraud Discovery Assets – and Watson?

IBM intends to build a portfolio of customizable, research-developed assets that use analytics to enterprise discover fraud, waste, abuse and errors in data intensive industries. These assets will be used to analyze internal data, to measure behavior, and find anomalies that indicate suspicious activity. These assets will be made available across industries for enterprise-wide discovery. And IBM's fraud discovery assets will be available on IBM SoftLayer-based clouds (as services). They will focus on medical fraud, insurance claim fraud, public tax fraud, and occupational fraud. Further, IBM plans to offer counter fraud as a service – including hosting, application management, behavior modeling & scoring and analytics and referral generation services.

For several years now Clabby Analytics has been following IBM's Watson cognitive computing environment. For those who don't remember Watson, it is a natural language based analytics engine that made a name for itself by beating two all-time revenue winning Jeopardy (game show) contestants. The way that Watson did this is by figuring out the statistical probability of an answer to a given question being correct – and Watson analyzed vast amounts of data to arrive at its conclusions. We at Clabby Analytics forsee a future role for Watson in counter fraud detection. Imagine a machine that can analyze vast amounts of data and queue-up anomalous findings. This would greatly simplify the job of discovery and make investigation easier to conduct. We believe that, over the next five years, the role of Watson in IBM's counter fraud offerings will increase – and we think this will represent a serious threat to black-hat bad guys the world over.

Summary Observations

Protection against fraud relies heavily on the time it takes to identify and remediate an attempted fraudulent activity. If enterprises had the time they need to examine each and every transaction that is submitted, then fraud would be greatly decreased. But we, as consumers, don't want our requests to complete transactions delayed – or worse, denied. And we want our medical and insurance claims paid promptly. And we want to use a wide variety of devices to initiate our transactions and submit our claims. Bad guys play on this need for speed to commit fraud.

As an electronically enabled society, we are all already paying for fraudulent activity – insurance companies, retail outlets, healthcare providers and others factor these costs into the products that they ultimately offer. And this situation is getting worse as black hats find new, innovative ways to break into systems and steal data. Aggressive actions need to be taken by enterprises and governments to stem this tide of dishonesty.

What IBM has done with its new Smarter Counter Fraud Initiative is it has created an architecture and accompanying services that can help enterprises prevent fraud as well as identify and overcome fraud. IBM has done this by integrating various sophisticated security and analytics tools – joining them together with IBM infrastructure offerings and linking them tightly with Big Data databases such that large volumes of data can be analyzed quickly. This is a huge step in the right direction to counter fraud because it puts in place a more effective, integrated architecture across which multiple tools can work together in concert to help identify and overcome fraud.

As several customers mentioned, there are still other factors that are preventing enterprises from building more effective fraud management systems. These include building one-version-of-the-truth databases; more effectively managing data; eliminating organizational silos; more effective inter- and intra-company collaboration; and better resource utilization. And, as always, growing the right skill sets is also critically important. We believe that IBM's Smarter Counter Fraud Initiative with its integrated analytics and management offerings will go a long way toward helping enterprises deal with all of these issues.

In the end, enterprises that are looking to stem losses due to fraud need to take a holistic approach to fraud prevention and management – and it is our opinion that IBM, with its Counter Fraud Management environment has architected such a holistic offering.

Clabby Analytics
http://www.clabbyanalytics.com
Telephone: 001 (207) 847-0163

© 2012 Clabby Analytics
All rights reserved
June, 2014

Clabby Analytics is an independent technology research and analysis organization. Unlike many other research firms, we advocate certain positions — and encourage our readers to find counter opinions — then balance both points-of-view in order to decide on a course of action. Other research and analysis conducted by Clabby Analytics can be found at: www.ClabbyAnalytics.com.