Managing the risk of fraud with Big Data in the banking industry, a consulting perspective

Stéphanie CANOVAS & Rim NAJI

Professor Mr. Kévin CARILLO

TBS Barcelona M2

OP Management Control & Governance

February 3rd, 2015

Acknowledgments

We would like to thank everyone who participated in the constitution of this research: first of all Mr Kévin Carillo, our mentor who oriented us and helped us in the delimitation of our subject. We also would like to thank very much each of our contacts and interviewees who trusted us and accepted to give us time and involvement in carrying out our study. Special thanks to Jérôme Pugnet, Director of GRC Solution Marketing at SAP who reviewed in advance our interview questions and answered in the best relevant way. We also express our gratitude to Chip Kohlweiler, Senior Manager Enterprise fraud management at Deloitte Atlanta (USA) who gave us relevant insight and ideas with his consulting perspective. Finally, many thanks to Philippe Besseyre des Horts, Executive Vice President Sales of Invoxis who accepted to give us a demonstration of their very innovative KYC solution.

Managing the risk of fraud with Big Data in the banking industry, a consulting perspective

Executive Summary

Nowadays, traditional methods of fraud risk management are still the most spreading ones in the banks. However, they struggle when facing the challenges of today's Big Data phenomenon: high-volume, high-velocity and high-variety of data. In this context, they tend to be inefficient and not flexible enough to adapt to the quickly evolving fraud threats. Big Data fraud management technologies appear to be the solution. These latest tools are able to leverage enormous volumes of diverse data in near real-time. This helps fraud departments to be more efficient, more accurate and to detect fraud that wouldn't be uncovered previously. Yet, we are still at an early stage of Big Data technologies and not every bank is ready to take this complex step. Indeed, it can be time and cost consuming to get full advantage of these newest solutions. It requires to centralize the bank's organization, to manage the change and to recruit the right team of skilled people. Besides that, it cannot replace some older methods such as relying on human intelligence. As banks are increasingly interested in Big Data solutions, it is an opportunity for consulting firms to step ahead and support their clients to face these new challenges.

Key words: Big Data; Banking industry; Consulting firm; Data analytics; Detection; Fraud management; Fraud schemes; Prevention; Regulation; Risk; Technologies.

Résumé

De nos jours, les méthodes traditionnelles de gestion du risque de fraude sont toujours les plus répandues dans le secteur bancaire. Cependant, il leur est impossible de faire face aux défis que leur impose le phénomène Big Data, caractérisé par les 3 « V » : Volume, Vélocité et Variété des données. Elles se révèlent alors inefficaces et inadaptées pour contrer les techniques de fraude qui ne cessent de se sophistiquer dans un tel contexte. Les nouvelles technologies Big Data apparaissent alors comme « la solution » car elles sont capables d'exploiter une volumétrie considérable de données variées en un temps record. Malgré tout, ces solutions n'en sont qu'à leurs débuts et ne sont pas encore accessibles à toutes les banques. En effet, il est complexe et coûteux d'en bénéficier tous les avantages puisque la banque doit notamment centraliser son organisation et faire appel à des professionnels qualifiés et rares. Aider les banques à faire face au Big Data dans leur gestion du risque de fraude s'avère donc une opportunité pour les cabinets de conseil.

Mots clés : Analyse de données ; Big Data ; Cabinet de conseil ; Détection ; Gestion du risque de fraude ; Technique de fraude ; Industrie bancaire ; Technologies

Table of Contents

INTRODUCTION

Organizations around the globe lose an average of 5% of their annual revenues to fraud, which account for around $3.7 trillion in losses. Fraud generally continues undetected for a median of 18 months and by the time it is detected, fraudsters are often long gone or losses are irrecoverable. (ACFE, *2014 Report to the Nations*).

Fraud is a wrongful or criminal deception intended to result in financial or personal gain (or causing financial or property loss). Fraud can be perpetrated by any employee within an organization or by those from the outside. It can generate important losses and damage the bank's reputation. That's why it is important to have an effective fraud management program in place.

Big Data is information of high-volume, high-velocity (speed of information generated and flowing into the enterprise) and high-variety (structured and unstructured data) that demand cost-effective, innovative forms of information processing for enhanced insight and decision making (Gartner, Inc.). This Big Data phenomenon is difficult to apprehend and to leverage as it requires the newest technologies. According to the Bank Info Security's *Faces of Fraud Survey* (2014), only 11% of banks are using Big Data analytics for fraud prevention.

Banking and financial industry tops the list of industries victims of fraud with nearly 18% of the cases studied in the *2014 Report to the Nations* (ACFE). The Big Data phenomenon has allowed fraudsters to use every time more sophisticated criminal tactics. This results in new issues for fraud investigators who struggle to pinpoint fraud across massive volumes of diverse and complex data. More sophisticated fraud schemes and the necessity to leverage Big Data for fighting fraud effectively explain the banks' eagerness to turn towards Big Data fraud management solutions. According to IDC Financial Insights, risk spending forecasts for the next few years will outpace growth in overall IT spending, representing over 18% of overall IT spending on average. This highlights the need for advanced technologies in the fraud risk management field in order to leverage Big Data.

"Managing the risk of fraud with Big Data in the banking industry, a consulting perspective": our title reveals the axes of this study, we will first explain the specificities of our research approach which also has an operational side, then we will discuss the current methodologies and tools used nowadays in the banks then try to show the role of big data in improving these tools for a better fraud risk management. To conclude we will expose the possible added value of the consulting firms in this improvement process.

1. METHODOLOGICAL CHAPTER

1.1. Study field delimitation

Cybercriminality has become a real business: according to Jacques Storch, In charge of fraud at the Crédit Agricole, “Cybercriminality has nowadays the turnover of both prostitution and drugs turnovers together”. This is a quite worrying statement when we know that we will have more than 2 billion computers connected in 2016, that we send 118 billion emails everyday, and that we are more than 1 billion facebook users and 19 million French using smartphones (*Study of IPSOS-CGI* for Elia Consulting 2013).

Our first research on the internet showed the existence of many R&D initiatives for each of these subjects, but much less for the two topics at the same time. Therefore, we have decided to cross “Big Data management” and “financial crimes” and go for the less covered part in research, not pretending a complete R&D project, but at least trying to think about these hot subjects and expose some lines of thought.

Why banks? They are the most exposed types of companies as they are a perfect entry point for criminals to reach people’s money and data. Especially when you know that 88% French trust their banks in protecting their personal data… On the other hand, banks are going towards dematerialization and fraud attempts are exploding, just for phishing the numbers of fraud trials is doubling every 4 months.

Depending on the way you look at them, these facts can be considered threats as well as opportunities: if there are threats for the daily customer and his bank, we can imagine that there are also opportunities for consulting firms who are in fact starting to help the banks in facing these news trends faster by making their action and clients secure. Indeed, if the banks adapt, that means that their tools have to adapt as well, especially when it is about a quite sensitive thematic like fraud.

Of course, legislation adapts to all that and a few years ago, the emergence of intelligence structures, the punishment for concrete fraud, the definition of monitoring frameworks and the several evolutions of law texts has shown the importance given to financial crime and fraud. The set-up of Bâle II in Europe, its transposition in France for instance through the 97-02 regulation, the growing authority of the dedicated instances such as the ACPR (“Autorité de Contrôle Prudentiel et Résolution”) or the “Commission Bancaire” reveals the necessity for French banks to take all the measures that frame the fraud risk management axes. These steps cannot be taken regardless to the changing environment in which we live and the opportunities presented by internet including the growing volume of data.

1.2. Research methodology and interviews of professionals

In order to shape our study and learn more about the subject, we have started by a research on the internet using appropriate key words such as “fraud management & Big Data”, “fraud management & data analytics” and other key words that we found all along our readings. We also searched on the legacy vendors’ websites which provide anti-fraud tools and softwares for the banking industry such as SAS, SAP, IBM, ACL...etc. Then, we used several data basis such as Business Source Complete and Xerfi in order to cross our sources and insure a good quality of information.

At the same time we have started to approach professionals in order to plan for interviews after deepening our research and preparing targeted questions. For this, we used our personal and professional network, professional events and also the professional network online: LinkedIn

Our professional network allowed us to meet Jacques Storch, In charge of the fraud at Crédit Agricole Sud-Méditérannée, which has accepted to tell us about the fraud risk steps and best practices. An interview with Florence Lebagousse, Norkom Project leader at the Crédit Agricole in Morbihan who gave us some general lines about the tools used in the banks nowadays.

Besides that, we have participated to the 20th national day of Economic Intelligence on December 11th. We have met Philippe Besseyre des Horts, Executive Vice President Sales of Invoxis, a software editor start up created in 2013, providing security and investigation services with advanced technologies. He gave us a demonstration of their very innovative Know Your Customer solution that leverage structured and unstructured data simultaneously with advanced text mining capabilities.

After reading the SAPinsider’s article *Detect Faster and Prevent Better with SAP Fraud Management* by Jérôme Pugnet and Tomás Kong from SAP, we contacted these professionals by email. Jérôme Pugnet, Director of GRC Solution Marketing at SAP answered to our questions with clarity and precision, and gave us relevant information from a solution provider’s point of view.

We also posted a document with our research plan and interview questions in several LinkedIn groups about fraud and Big Data as well as on slideshare (sharing slides via linkedIn). In less than two weeks, we got 400 documents’ views and a few downloads. This allowed us to be directly contacted by several professionals interested in the topic.

We interviewed Chip Kohlweiler, Senior Manager Enterprise fraud management at Deloitte Atlanta, USA. Well experienced in the area of Fraud and Big Data in the banking industry, he gave us interesting ideas and plenty of insight about how consultants help banks managing the risk of fraud in a context of Big Data expansion.

We have also participated to a webinar organized by Integrc (company that provides Governance, Risk management and Compliance services to companies that run SAP) and entitled "How SAP Fraud Management ensures you avoid modern fraud-related". We then tried to complete our information thanks to other webinars posted on YouTube.

Since we have adopted several methodologies of research, we have encountered two main constraints. We have noticed through our documentary research the limitation of research articles linked to Big Data as a way to manage the risk of fraud. We confirmed this fact with the professionals that we interviewed. According to the discussions we had, this may be strongly linked to the newness of the topic in the field of research.

Also, given the sensitiveness of the subject we encountered real difficulties to know how some banks react with fraud risk. Many professionals we contacted declined for confidentiality reasons, even if it was about the methodologies and not concrete cases, the IT strategy applied to fraud stays a very sensitive subject. That was also what we noticed with some professionals who accepted our interviews. For these reasons, we could not go into the details of the existing processes and we wish we could know more about the future tools and strategies of the Banks. Even though, we have succeeded on tackling this issue by compensating with interviews in the consulting field and knowing about the tools of the market which are designed for the banking industry.

2. Traditional fraud risk management solutions are still the most widely used methods in the banks but they tend to become weak in a context of Big Data expansion

2.1. A strong fraud risk management system

Fraud is an intentional act that aims to obtain a material or intangible benefit to the detriment of a person or an organization, committed in contravention of the laws, regulations and internal rules, or infringing the rights of others, or concealing all or part of an operation or set of operations or some of their characteristics.

Generally, we can identify three kinds of fraud: internal, external or mixed fraud.

External fraud is committed by individuals, singly or in groups, clients or not, acting in their identity under a false identity or through a corporation, to obtain funds, documents or information used to their advantage to act to the detriment of an entity (bank) or its customers or third parties. Internal fraud involves the active or passive participation of an employee of the entity (bank), either exclusively or in collusion with outside individuals (mixed fraud). Internal fraud also includes unfair behavior of collaborators resulting in intentional breach of the duties performed, granted delegations and rules defined by the entity in each business area: it is, for the activities of markets, including cases of Positions / unauthorized transactions or out of bounds transactions which are initiated intentionally or concealed.

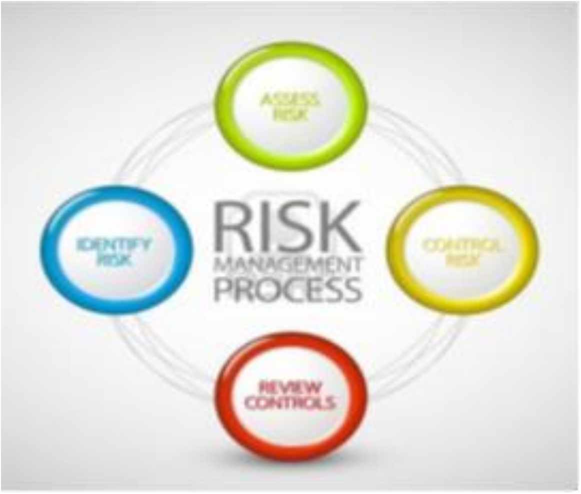
Fraud can take many forms, going from fiscal fraud, to payment tools or corruption:

Banking/Financial Services - 298 Cases

Scheme	**Number of Cases**	**Percent of Cases**
Corruption	101	33.9%
Cash on Hand	64	21.5%
Billing	37	12.4%
Check Tampering	35	11.7%
Non-Cash	33	11.1%
Skimming	32	10.7%
Larceny	29	9.7%
Expense Reimbursement	20	6.7%
Financial Statement Fraud	16	5.4%
Payroll	9	3.0%
Register Disbursements	8	2.7%

Distribution of Fraud Schemes in Banking/Financial Services

2010 Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse, Association of Certified Fraud Examiners



The risk management process in a bank is crucial and banks are more and more careful to their anti-fraud strategies.

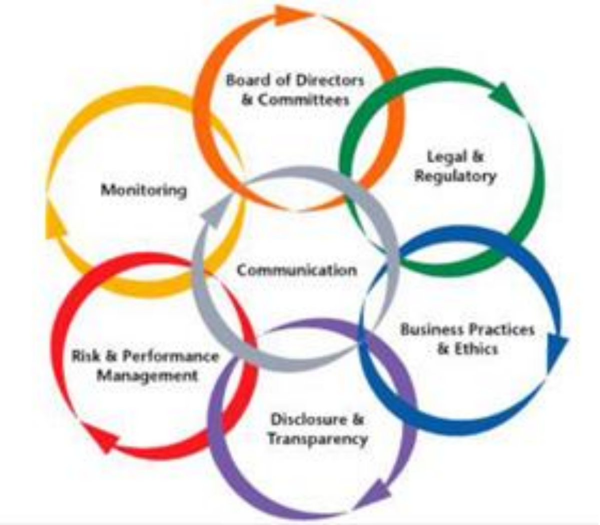
In fact, implementing a fraud risk management process in a bank has several aims:

First, reducing the risk of exceptional fraud:

- Improving the prevention and deterrence of attempts,
- By providing faster detection of fraud (facilitating the recovery of misappropriated funds)

Second, ensuring a better control of recurrent fraud in volume and value

Third, adapting control and detection systems (also through technology).


Board of Directors & Committees
Legal & Regulatory
Monitoring
Communication
Business Practices & Ethics
Risk & Performance Management
Disclosure & Transparency

Globally, it is about limiting the costs of fraud by strengthening prevention and control systems as well as the involvement of all the stakeholders. To reach these objectives, management has a real responsibility to ensure the monitoring of behavior of its employees with increased vigilance for sensitive functions (such as the front office) and respect the general professional rules (compliance of IT authorizations, protection of company data etc).

For these reasons, a strong fraud risk management system is absolutely necessary; it is also a real prevention from reputational damage and heavy sanctions. Fraud can happen in every bank even the biggest and the Bernie Madoff Scandal has shown that. In 2008, Bernard L. Madoff Investment Securities LLC was a Wall Street investment firm founded by Madoff. Bernie Madoff, his accountant, David Friehling, and Frank DiPascalli tricked investors out of $64.8 billion through the largest Ponzi scheme in history. Investors were paid returns out of their own money or that of other investors rather than from profits. Madoff was arrested the next day and got penalties of 150 years in prison for Madoff besides a $170 billion restitution and prison time for Friehling and DiPascalli.

2.2. An overview of Fraud risk management methodologies in the French Banks

In order to manage fraud risk, French banks establish first an adapted framework for the entity's governance and values. Establishing an anti-fraud chart, creating the corresponding organization (fraud cell, financial security department, compliance department, internal auditors, permanent controllers etc), giving "the tone at the top", and communicating around the risks of fraud are the first steps to take in parallel with the strong controlling system discussed in the previous part. Also, banks explain the risks for the bank in case of fraud occurrence and the sanctions for an employee in case of taking part in an internal or external fraud scam-this is mainly achieved through the bank's value communication and the trainings.

Traditionally banks also rely on the "Know Your Customer" (KYC) concept as a basis for managing the risk of fraud. KYC relies first on the identification and the verification (ID, official address, activity etc) of the prospect before he becomes a client.

This first step has to be enforced by proofing documents and details by mentioning the nature and the object of the relationship. Generally, the bank has to know about the expected use of the account in order to define the risk profile of the client. In France, checking the identity and characteristics of the client is compulsory by law before entering in a relationship (article L561-6 al.1 Code Monétaire et Financier) and during the relationship with the client (article L561-6 al.2 Code Monétaire et Financier). In order to grant a good KYC, the client data has to be updated on a regular basis, with the necessary and compulsory documents besides that, the bank has to know about the origin and the destination of the funds and ensuring the coherence between the client profile and his financial transactions.

Unlike what is common to think, whistleblowing is often not taken seriously by fraud professionals, unless the content really deserves a real enquiry and contains proof. By contrast, alerts generated by monitoring tools are given much more time and analysis. In fact, banks have tools which help in detecting potentially fraudulent transactions, often by generating alerts showing an unusual transaction considering for instance the habits of the clients or his average transactions.

Norkom Technologies is a leading player in the financial crime and compliance market sector. Norkom enables many banks in France and internationally to fight crime and meet the most stringent demands of the regulator with a portfolio of products that address every aspect of crime and compliance - from money laundering to fraud. The alerts generated by such a tool will be analyzed and completed by the knowledge the bank has about the client, his transactions history, the relationship manager opinion, extractions by other softwares of the bank, in different databases, on the internet, by getting complementary documents and every other adapted source of information. The analysis may be completed by softwares such as eFIRST which is often used to capture, sort, process checks and scan them-or by internet platforms like RESOCOM which helps to reveal the extent of identity fraud from private economic actors and public authorities certifying the control of identity supports.

To detect fraud, banks also use data analytics: processes and activities designed to obtain and evaluate data to extract useful information and answer strategic questions. Several ways to leverage data are by: vendor attributes analysis, trending of vendor activity (acceleration, valley, or spike patterns), name mining, overtime & vacation hours' analysis or identification of "high-risk" payments or checks issued on weekends. Data can be found in the vendors & accounts payable, claims, employees & payroll, expense reimbursement, travel & entertainment and in the General Ledger. To best use data analytics, banks try to assess risk, define clear objectives, obtain the necessary data, develop and apply procedures, analyze and finally manage results.

2.3. Limits of the traditional solutions in a context of Big Data expansion

The methodologies used in the banks and mentioned before, show the need for banks to cross several sources of information even if they have a tool for detecting suspicious transactions. This can be time and energy consuming. Also, the alerts generated are based on the internal database of the bank which leads to complementary research on the internet in order to get external data. In reality, the analysis made in banks is based on a procedure to follow by different anti-fraud collaborators; this makes fraud risk management on their hands. Therefore, the analysis can be very subjective and depends on the view or on the experience of the person in charge of the field analysis. It can also depend on the completeness of the information the bank has about its client.

Big Data" is a growing and new challenge that banks have to face. This phenomenon is often described by three "V": high-volume (the amount of data), high-velocity (the speed of information generated and flowing into the enterprise) and high-variety (the kind of data available) information assets. These characteristics are difficult to manage with traditional processes or tools. Indeed, banks can amass petabytes of information in a year and traditional tools struggle to leverage such enormous volumes of data. In addition, traditional methods cannot go as fast as the thousands of credit card transactions occurring every second and loss will occur before anything could be done. Finally, many estimate that 80 percent of data is semi-structured or unstructured. Structured data reside in a fixed field within a row-column database but unstructured data refer to data that can't fit neatly in a database (e-mail messages, word documents, videos, photos, audio files, webpages…). The latter is near-impossible to analyze with traditional methods. Without being able to leverage Big Data banks are missing significant opportunities to prevent and detect fraud.

Traditional methods tend to be inefficient in an increasing complex environment driven by Big Data expansion. Indeed, Chip Kohlweiler, Senior Manager Enterprise fraud management at Deloitte explained that Big Data intimidate banks. They have already invested tens of millions of dollars in technologies and don't even know how to leverage them. In fact, banks struggle with the "where to start?" question. Moreover, one of the banks' main concerns with traditional methods and tools is that they generate lots of false positives and negatives. They have so many cases to investigate that it is time consuming and it ends up in huge amount of suspicious transactions backlog. Besides that, these methods use a reactive approach that relies on an "after the fact" analysis, which doesn't help the banks to prevent effectively the fraud. This generates even more fraud cases to analyze.

Traditional tools are not flexible enough to adapt to the changing environment and fraud schemes. Attackers have become increasingly creative about devising new methods to fraud which makes the detection harder and the analysis more complex for each fraud case. Jérôme Pugnet, Director GRC Solution Marketing at SAP explained that one of the limits of traditional tools is that they are not flexible and banks struggle to change the rules in order to adapt to the new fraud schemes. Therefore, when fraudsters' tactics evolve quickly, banks can't respond in time.

New technologies are evolving in this direction, and many institutions have brought information security professionals into the boardroom. Whether they have a Chief Risk Officer (CRO) or Chief Information Security Officer (CISO). Nowadays, managers realize that Big Data and its real-time intelligence abilities are strong assets if the insights they enable are quickly available to be applied through new processes, risk rules, and defense mechanisms.

"Data and analytics tools will undoubtedly create new opportunities for improving risk detection and prevention, so it's never been more critical for financial institutions to continue their leadership in adopting these technologies to stay a step ahead of cyber criminals." Mike Gross, Global Risk Strategy Director at 41st Parameter.

3. Big Data technologies as a big opportunity for fraud risk management in the banking industry

3.1. Big Data solutions seem to be more appropriate nowadays

Big Data solutions address the challenges of the "three Vs" where traditional methods struggle: Volume, Velocity and Variety of data.

The first challenge for traditional tools is to deal with enormous volumes of data as banks can generate terabytes of new data every hour. Most of banks work with data volumes that do not correlate with the relevant size of their business (*Global Forensic Data Analytics Survey,* 2014, Ernst & Young). They often use data sampling which is ineffective when it comes to finding fraud. Most frauds are not noticeable in sampling. To be effective in fraud detection, banks have to leverage the complete data set. This is possible with Big Data tools that enable banks to analyze all the data set available to the bank. Hadoop, which is a framework that processes large data sets across clusters of computers, is one of the main tools able to leverage such a massive amount of data streams.

The second challenge is to detect or even prevent fraud in a high-velocity data environment. Banks have to analyze transactions as quickly as they occur to take immediate corrective actions in case of threat. To do that, they have to process data in near real-time. When this is not possible with traditional methods, sophisticated tools can integrate advanced analytics such as predictive modeling that will flag or stop fraudulent transactions much sooner and before any damage is done. As the speed of information generated is increasing, fraudsters are able to evolve and adapt their tactics quickly. To fight these rapidly changing fraud schemes, banks need tools that enable them to be flexible and adjust to these schemes. Jérôme Pugnet said that SAP Fraud management solution powered by the Big Data technology SAP HANA which is based on in-memory capabilities, can leverage and process high volumes of data quickly. The solution can detect and block a suspicious transaction in near real-time. An alert is then sent to an investigator for analysis. SAP solution also allows banks to customize and adapt the solution to evolving threats by changing the rules to the new requirements.

The third challenge is to be able to analyze structured and unstructured data simultaneously when most of data is semi-structured or unstructured. Indeed, this type of data is very difficult to analyze and time-consuming with traditional methods that are limited to the analysis of structured data. The ability to analyze text and other unstructured data can give lots of insight to the bank's fraud management. It can spot criminals who can hide behind the structured data: forwarding sensitive information to a personal email account for instance. A good example of challenging unstructured data analytics for fighting fraud is text analytics. It is the process of structuring text using different techniques and algorithms for detecting patterns and connections in the text. As text is open-ended and can be interpreted in numerous ways, analysts need to start with hypothesis and know what they are looking for in the text, which is not easy to shape accurately. SAS® Text Analytics for instance, is a solution that automatically assesses, analyzes, understands and acts upon the insight buried in electronic text. But what banks are seeking now with Big Data solutions is being able to harness both structured and unstructured data that exist in different locations simultaneously. It allows the bank to get a full and accurate view of the enterprise and detect more fraud schemes such as collusive relationships.

3.2. Importance of reliable Big Data tools for an efficient fraud risk management

Big Data tools enable banks to be more efficient in their fraud risk management. Traditional tools and methods can be time consuming and have limitations in doing analytics with Big Data. On the contrary, Big Data tools harness data at speeds once inconceivable. It accelerates the processes giving the company access to data in real-time. What would have taken weeks or months for investigators can now be done in minutes. For example, Ernst & Young explain that thanks to IBM Big Data platform, they could reduce their clients' query time from 4.5 hours to just 2 mins 30 sec. In the *Global Forensic Data Analytics Survey,* 2014 of Ernst & Young, 47% of respondents who use only spreadsheet or database applications in their Forensic Data Analytics efforts report analyzing the free-text payment descriptions in the accounts payable fields to identify potentially improper payments. Manually analyzed by an investigator, it can be very inefficient and time becomes a major inhibitor. Thanks to Big Data tools such as text analytics and mining, this becomes possible: it generates efficiency, uncovers fraudulent tactics quickly and ensures that legitimate transactions are processed without delay.

Besides that, Big Data solutions tend to be more accurate. Managing Big Data with traditional methods doesn't allow for the level of scrutiny and analytics that is needed to detect the most hidden fraudulent activities. Key connections can be missed. On the contrary, Big Data tools are more accurate as advanced algorithms can be developed to be more precise and reduce false positives and negatives. This accuracy leads to less cases to analyze but better qualified, which also means time-savings. Banks can more accurately define what risk areas they have to monitor and invest time and money on. Big Data solutions can also be able to find the figurative “needle in a haystack” that may represents major fraud threats.

Big Data tools tend to have limitless capabilities and integrate an increasing number of useful applications such as visualization and social network analysis. As we have seen, they allow banks to leverage and analyze tremendous volume of diverse data in near real-time. This helps banks to minimize the zone of ignorance and detect frauds that wouldn't be uncovered previously. To derive even more insight from Big Data, some technologies offer the capability to visually analyze data. Visual representations illustrate the story behind the data and demonstrate connections that are not obvious between people, places and things. This gives the bank a holistic view of interconnections between accounts and transactions across channels and products and for a network of individuals. Visualization is also a powerful and insightful tool for communicating fraud cases to management, fraud investigators or law enforcement. Moreover, being able to derive insight from Big Data is enhanced by Social Network Analysis (SNA) capabilities. The Fraud Management Institute explains that “SNA develops a complete picture of any fraud event by finding specific entities (individuals, accounts and transactions) that may be involved in fraud and then establishes links between these suspect entities and other entities that may be related. Once the links are constructed, they need to be refined with analytical techniques to produce meaningful networks that have a high likelihood of actual or potential fraud.” In other words, “it connects the dots between apparently isolated clues that, when interlaced, can create a picture of the overall fraud scheme.” SNA platforms can be powerful at providing a full enterprise view of fraud threats whose tactics span various channels, product lines and countries. However, SNA is not new but what changes is the emergence of capabilities to construct networks automatically and leverage Big Data.

3.3. Big Data solutions tend to be more beneficial and least costly

Traditional methods provide reactive analysis of suspicious transactions, which doesn't protect from loss. Indeed, the earlier the bank uncovers the fraud the greater its chances are to stop the fraudster before any incident and minimize the associated loss. That's why, Big Data tools tend to be proactive, predictive and preventive thanks to their advanced and automated analytics capabilities that allow continuous monitoring. This helps banks to take more informed and anticipatory decisions. These abilities tend to discourage fraudsters to attempt any crime and seek an easier target.

Jérôme Pugnet explained that SAP Fraud management is often used with SAP Predictive Analysis, which allows banks to create new and more advanced algorithms in order to predict future fraud activities. He also highlighted that if there is fraud it is often because of a weak control environment. Continuous monitoring helps detect weak controls and give key insights to internal auditors for improving existing controls or creating new policies. Effective controls can be powerful in preventing frauds.

Beyond the detection of fraud, banks have to remain compliant in an increasing regulatory environment to prevent engaging in fraudulent activities themselves. The recent BNP Paribas's “Tour de Fraud” breaking US sanctions against trade with Cuban, Iran and Sudan is a good example of non-compliance. The bank has to pay a fine of 9 billions of dollars and this event damaged its reputation. Governments around the globe have introduced policies such as Know Your Customer (KYC) and Enhanced Due Diligence (EDD) to prevent fraud and money laundering. As these regulations change from country to country, it is difficult for banks to have an overall view of a customer across geographic regions. However, to avoid large fines and reputation damages, banks have to improve their KYC processes to meet regulatory requirements. Banks should be able to detect potential criminals among individuals they do business with or want to do business with and regularly update their profiles as events occur.

Philippe Besseyre des Horts, Executive Vice President Sales of Invoxis gave a demonstration of their KYC solution. This innovative KYC visual platform can analyze structured (banks' CRMs and IS...) and unstructured data (Web, social networks...) simultaneously and leverage advanced text mining capabilities. It can give plenty of insight about individuals and companies with who banks are doing (or want to do) business and answer questions such as “is this company recorded in a list of sanction?”.

Big Data tools have capabilities to uncover new fraud schemes on the contrary of traditional methods. In fact, the latter struggle to watch consumer behaviors across product lines, channels, systems and geographic areas. Indeed, this approach works channel by channel or region by region, which is too slow and inefficient for an early detection of threats. Fraudsters already know this weakness and take advantage of it. Indeed, instead of setting a large one-time attack that could be uncovered, they do lots of small activities in multi-areas. Fraudsters are evolving from individual attacks to very organized and decentralized tactics. They also go to new banking channels where controls are not yet strong enough such as electronic banking (online, mobile and other e-channels).

4. […] But Big Data solutions are not yet usual nor accessible to every bank

4.1. The cost of implementing Big Data tools is still high

Implementing a Big Data solution is a major decision, as it is time and cost spending to get the right information. In the *Global Forensic Data Analytics Survey* of Ernst & Young (2014) “72% of respondents believe that emerging Big Data technologies can play a key role in fraud prevention and detection. Yet only 7% of respondents are aware of any specific Big Data technologies, and only 2% of respondents are actually using them”. Banks are aware of the Big Data phenomenon and its potential benefits for fraud management but they lack specific information to decide about implementing any of the Big Data solutions. As we have seen previously, banks already struggle to get full advantage of their current systems and lack of information about Big Data tools, which are even more difficult to apprehend, they are not feeling ready for implementing more advanced solutions. Moreover, today we are still at an early stage of Big Data solutions and banks are waiting for more proof of concept. For example, SAP has released its SAP Fraud management solution powered by the Big Data technology SAP HANA only one and a half years ago. IT investment is most of the time a strategic decision taken by a Chief Information Officer who builds a several years plan and it takes time to make such a decision and invest in Big Data.

Prior to any Big Data technology implementation, a bank needs to centralize its organization. Chip Kohlweiler explained that Banks often operate in silos. They can have commercial and consumer banking fraud departments completely separated and using completely different technologies. It doesn't make any sense but it is often the result of their historical growth through mergers and acquisitions and their focus on customer satisfaction. Indeed, in many large banks, each line of channels (credit cards, online banking...) has a team of people that may have differing objectives and who use different tools and processes. With this siloed approach to fraud management, the bank's different groups cannot communicate well to each other and will miss relationships between channels. However, Jérôme Pugnet put forward that an important prerequisite for implementing SAP HANA or even create synergies in managing fraud, is to centralize the bank's organization. To successfully implement a Big Data solution, it has to be integrated in the overall system. For that, banks have to first coordinate their fraud management departments. Reorganizing is not a quick and easy task.

As most of Information technology investments and implementation, Big Data solutions are costly. First, they are based on sophisticated technologies and banks have to pay the price to get such advanced technologies and replace some of their existing technology and infrastructure. This expense often doesn't fit in the budget. Then, even if many Big Data technologies can be integrated in the bank's overall Information System which contain massive amount of valuable data (CRMs, ERPs...), this is always complex to implement, customize and integrate a new solution. For large banks it is often a multiyear project with an important change management. Since it is often too costly to implement a Big Data solution, IT managers first think of what they could improve and get full advantage of their existing fraud management tools such as integrating additional data or predictive capabilities.

4.2. Challenge of getting full advantage of Big Data technologies

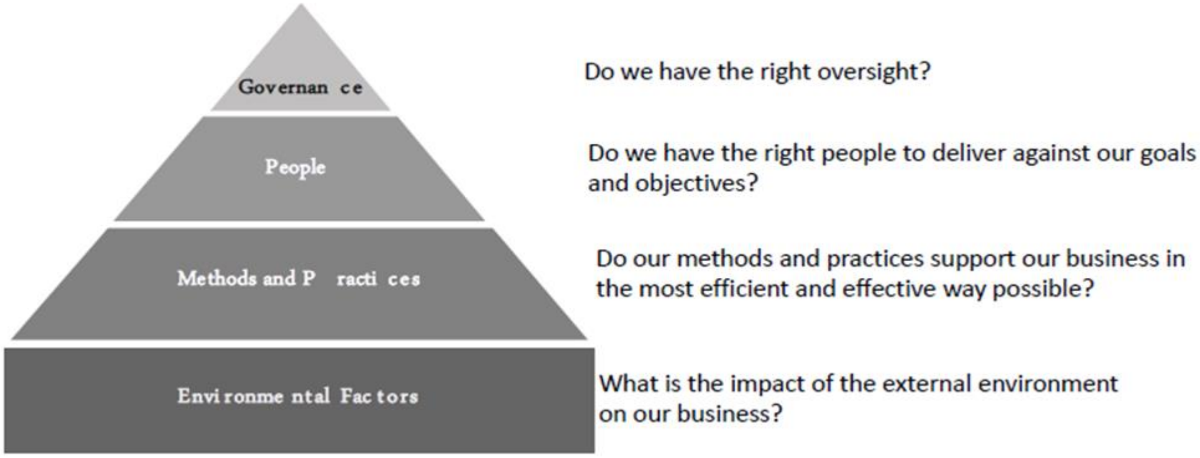
Implementing a Big Data solution is only one key success factor to effectively fight fraud in today’s context. Another equally important key is to recruit a team of experts such as data scientists who know how to get advantage of the Big Data technologies. These professionals know what data is available, how to leverage it and what to look for in the data to detect any fraud. A regular business analyst won't necessarily know what fraudulent activities look like in the data. Chip Kohlweiler explained that they recommend to their clients to have a team of data scientists to support the fraud management system. Banks need the right skilled people to keep the fraud management system going on in the long term without having to rely on external consultants. Data scientists can continuously review the models and adapt them regularly to the new requirements. However data scientists can be scarce and are expensive to attract and retain. Sometimes, it is even better for banks to hire more staff to work on more alerts as new fraud activities are detected and prevent losses. In addition, banks have to make sure they have someone senior on board such as a Chief Information Officer or a Chief Data Scientist who are expert in new technologies and can make the right decisions.

Another concern of implementing Big Data solutions is “what will be the impact of the new tool on their customers?” Banks don't want that these sophisticated tools generating a higher security system to hinder the customer’s banking experience during the implementation and after. Banks are always in a dilemma about whether or not putting painful controls for customers to prevent fraud.

Leveraging Big Data leads to data privacy issues because being able to collect larger set of data regardless of where they are hosted and use them with near-limitless capabilities make violation of privacy easier. In addition, privacy and information security laws differ from one country to another and are even evolving more rapidly these last years in result of the Big Data phenomenon. That's why it is important to implement a security and privacy strategy to prevent any abuse or data breach and preserve the customer's trust in the bank. The Chief Security Officer or Chief Information Security Officer should make the right decision to manage data privacy issues. He should ask himself the questions: How can we protect the customer's privacy? What data do we collect? Are these data sources protected? Who can have access? How to use these data without abuse?

4.3. Big Data solutions cannot replace traditional methods and finding fraud still relies on human intelligence

Big Data tools are powerful tools indeed, but can we say that they can replace human intelligence? If that was the case, how to analyze unique fraud cases? How to ask the right questions at the right moment? Managing the fraud risk is about all of governance, people, methods, practices and environmental factors. Here, a Big Data solution would only answer to the “methods and practices” layer.


Governance
People
Methods and Practices
Environmental Factors
Do we have the right oversight?
Do we have the right people to deliver against our goals and objectives?
Do our methods and practices support our business in the most efficient and effective way possible?
What is the impact of the external environment on our business?

One should also remember that fraud detection and prevention starts at the client level, the education of the client for an adequate use of the payment tools and his sense of discernment are the first qualities which cannot be replaced by a tool, even a Big Data tool. Also, the bank advisor (the relationship manager) plays a crucial role in appreciating the profile of the clients, his needs, his habits, his reactions and the general feeling established. Fraud risk management is a concern for each employee of a bank from the welcoming desk to the accountant as well as at the fraud department members' level. "There are some effective approaches that highlight how putting the right information in front of the appropriate team can make a world of difference" said Mike Gross, Global Risk Strategy Director at 41st Parameter. This shows that the tool that transforms raw data into useful information is a wonderful asset but it can lose its value if it is not used as it should and by the right persons. Jérôme Pugnet added that we cannot replace highly experimented investigators who can find fraud where no one would have noticed it, even with advanced technologies.

5. What Consulting firms can use from our study

5.1. How can a consulting firm help its client to manage fraud risk in a context of Big Data expansion?

When banks ask for consulting services for their fraud risk management, it is because they need help and advice from informed professionals. That's why, consulting firms must keep up to date. They have to be aware of changing environment such as bank regulatory requirements, evolving fraud schemes in the banking industry and latest fraud management solutions in a context of Big Data expansion. For instance, if the concept of Big Data is new for the bank, they have to be able to define it and explain how to leverage it. For instance, Jérôme Pugnet said that SAP has released its latest Fraud management solution adapted to the banking industry only 3 months ago. It is derived from the main solution but it contains predefined rules and other content relevant for the banks. SAP co-developed this solution with large banks and specialized consulting firms.

Banks also expect from consultants an effective assessment of their current fraud management. Consulting firms have to be able to bring out any dysfunctions, how to get full advantage of the existing system or its limits. The latter could lead the bank to update or change its current fraud management. Each consulting firm who works on enterprise fraud management has its own methods to assess bank's fraud system. However, here are some of the main points consultants should take into account:

- How the bank is organized, what are its processes and controls? Are they effective and is there any weakness?
- What are the high risk areas and does the existing fraud management address them?
- Does the system generate many false positives and negatives?
- Are potential frauds being missed?
- Can the system expand or adjust to the changing fraud schemes?
- What are the data available and what data is the system able to leverage?
- Does the bank get full advantage of its existing solution?
- How to improve the existing fraud management (adding predictive analytics...)?

- Benchmarked against latest technologies available on the market, what are the gaps?
- Does the bank have an effective continuous monitoring and improvement fraud management? Does it have an effective feedback loop?
- Does the solution allow the analyst to create and develop a fraud case in order to investigate and communicate effectively (data visualization...)?

Consulting firms have to define what fraud management is best adapted to the bank situation. Big Data solutions can generate lots of benefits in managing fraud but we have seen that only a minority of banks are effectively using them. In fact, many are not ready for the Big Data challenge because of the cost, the complexity or the change in the organization it needs prior to the implementation. Consulting firms have to adapt to the bank's strategy such as budget restriction or IT decision and find the best suited fraud management for the bank. For example, if the bank doesn't want to avoid cost of hiring data scientists or programmers, consulting firms should advise easy to use Big Data platforms in the Cloud from providers such as SAP or IBM. In addition, to complete their existing fraud risk management, consultants could also tell the bank to rely on startup services such as Invoxis that provides effective KYC and Due Diligence services at unbeatable prices.

5.2. What Consulting firms should take into account while implementing a Big Data fraud management solutions

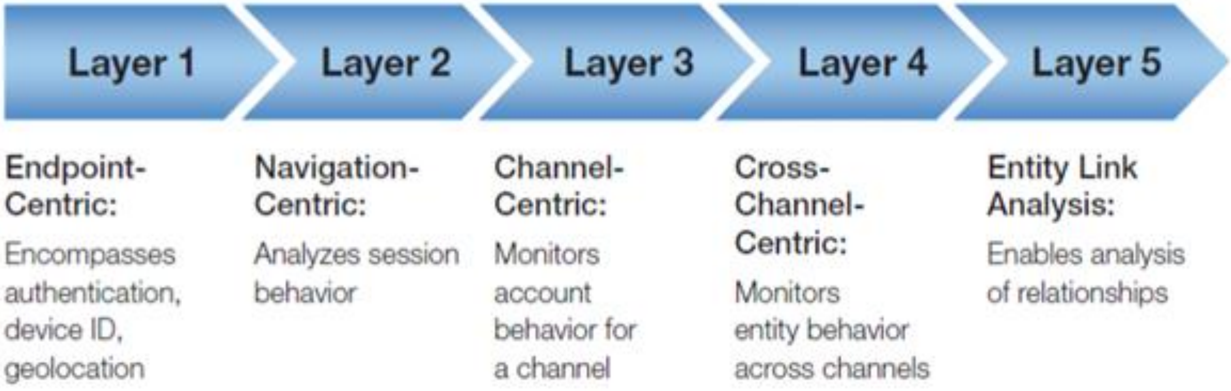
Most of the time banks track fraudulent activities in silos which is not giving them the full picture as fraudsters operate more and more like organized fraud rings. To fight fraud better and implement a Big Data solution efficiently, consulting firms should advise banks to go from a decentralized organization to a more integrated approach. Thanks to this enterprise approach banks are able to detect fraud that would not be uncovered previously.

Chip Kohlweiler explained that banks generally have solutions that cover all of the schemes but they often don't know where to start and how to start small. He put forward a relevant idea that is to start with a pilot project. This pilot project should be something small enough, tangible enough, and easy enough to digest and start with. When they get a proven success with this project they can grow from there. Therefore, consulting firms should be able to help their clients to start small, define a roadmap with priorities and build a coherent project plan. An enterprise-wide deployment is a multiyear project.

We have seen that even if many vendors try to develop user-friendly platforms for regular business analysts or investigators, having the right team of skilled people to support Big Data technology is necessary to get full advantage of it and develop advanced analytics. That's why, consulting firms must explain to their clients that the best way to leverage Big Data solutions' benefits, it is to recruit the right team of experts such as skilled investigators and data scientists to keep the fraud management going on in the long term and to have senior-level executives on board who can make decisions.

5.3. A layered approach for fighting fraud

A common and easy framework for an effective fraud management is prevention, detection, investigation, report and a feedback loop. However, we will highlight an interesting approach for fighting fraud in a context of Big Data expansion developed by Avivah Litan from Gartner, Inc: *The conceptual model of a layered approach to fraud detection* (below). That framework has been a hot topic at the 2012 Association of Certified Fraud Examiners Annual Conference in Orlando, USA.


Layer 1
Layer 2
Layer 3
Layer 4
Layer 5
Endpoint-Centric:
Encompasses authentication, device ID, geolocation
Navigation-Centric:
Analyzes session behavior
Channel-Centric:
Monitors account behavior for a channel
Cross-Channel-Centric:
Monitors entity behavior across channels
Entity Link Analysis:
Enables analysis of relationships

Conceptual model of a layered approach to fraud detection, as described by Avivan Litan, Gartner Group.

As no single control is enough to fight new fraud schemes such a cyberattacks, a multiple levels of controls framework with multiple analytical capabilities will provide the bank a defense in depth. Ms. Litan said that implementing such a system take several years and she recommends to start deploying first the lower levers of the layered approach to fight immediate threats and progressively deploy the upper levels that take more time to implement.

CONCLUSION

Nowadays, traditional methodologies of risk fraud management are the most spreading ones in the majority of banks. Indeed, fraud services still rely on classical tools which allow an ad hoc approach and which need to cross several sources of information. But, in a context of Big Data expansion, these traditional methods struggle with three main challenges: high-volume, high-velocity and high-variety of data. Therefore, banks' traditional fraud management generates lots of false positives and can't adapt to the evolving fraud schemes.

New Big Data technologies seem to be the solution. These tools are able to leverage enormous amounts of diverse data in near real-time giving the bank much more insight. This helps fraud services to be more efficient, more accurate and to detect fraud that wouldn't be uncovered previously. Besides that, when traditional methods only are reactive, Big Data solutions tend to be proactive, predictive and preventive, which can more effectively stop fraudsters before any damage is done. That's why banks are more and more going towards Big Data technologies.

However, Big Data solutions are not yet usual nor accessible to every bank. Implementing this newest technology can be time and cost spending. Prior to any implementation, banks have to get the right information and centralize their organization and after, they have to succeed their change management. Getting full advantage of Big Data technologies also requires recruiting the right team of skilled people and managing customer experience and international data privacy issues. In addition, these new solutions cannot replace some effective characteristics of traditional methodologies and especially human intelligence.

As banks are increasingly interested in how to leverage Big Data, they often ask support and advice from consulting firms. That's why, consultants must keep up to date with this hot topic and with the latest technologies. As many banks are not ready for the Big Data challenge, consulting firms have to assess their clients' fraud system accordingly and define what fraud management best suit them, Big Data oriented or not. When the decision is taken to implement Big Data technology, consulting firms must remember that their clients must start small, with a pilot project. Banks can then grow from there and build a robust, enterprise-wide Big Data fraud management with several layers of controls.

BIBLIOGRAPHY

ACL (2014), *Fraud detection using data analytics in the banking industry*, Discussion whitepaper

Autorité de Contrôle Prudentiel et Résolution (2014) [online] : http://acpr.banque-france.fr/fileadmin/user_upload/acp/Controle_prudentiel/reglt97-02-consolide.pdf

BARTA Dan, STEWART David (2012), *A layered approach to fraud detection and prevention*, Conclusions paper, SAS

Capterra.com (2014), *List of Financial Fraud Softwares* [online]: http://www.capterra.com/financial-fraud-detection-software/

CLOPTON Jeremy (2014), *Bank fraud prevention and detection – The case for Data Analytics,* BKD Webinar: www.youtube.com/watch?v=p93wm5lvqek

CLOPTON Jeremy (2013), *Detecting fraud through Data analytics, BKD Webinar*: www.youtube.com/watch?v=hDaCJuk-vo0

Code Monétaire et Financier (1997/2010), *Règlement no 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement*, Law text

DANN Anthony Maurno (2013), *The latest Fraud-Finding Tools*, Article Compliance week

Deloitte Forensic center (2013), *Using analytics in banks, smarter continuous monitoring*, Article, ForThoughts Deloitte newsletter

Ernst & Young (2014), *The perfect storm*, Article

Ernst and Young (2014), *Big risks require Big Data thinking*, Global Forensic Data Analytics Survey

GRIFFIN Robert (2012), *Using Big Data to combat enterprise fraud,* Article Financial executives

HARRIS Sam (2012), *Teradata enterprise risk intelligence for fraud and financial crimes prevention*, Whitepaper, TERADATA

IBM Corporation (2014), *IBM Counter Financial Crimes Management for Banking*, Solution brief

IBM Corporation (2010), *IBM Infosphere Biginsights*, Solution brief

Integrc (2015), *How SAP Fraud Management ensures you avoid modern fraud-related*, Webinar

Intel, IBM (2013), *Combat credit card fraud with Big Data*, Whitepaper

ISACA (2011), *Data analytics - a practical approach,* Whitepaper

JAEGER Jaclyn (2014), *Using Big Data to Find Fraud? First, Find the Data*, Article, Compliance week

Javelin Strategy & Research (2012) *Current State of E-channel fraud trends: online banking, mobile banking and card fraud*, Whitepaper, SAS

LITAN Avivah (2011), *The five layers of fraud prevention and using them to beat malware*, Research Report

MEHRA Gagan (2013), Using Big Data to prevet Ecommerce fraud [online]: http://www.practicalecommerce.com/articles/4031-Using-Big-Data-to-Prevent, Ecommerce-Fraud-

Observatoire BDF (2011) La coopération internationale en matière de luttre contre la fraude, Press release : https://observatoire.banquefrance.fr/fileadmin/user_upload/Observatoire/pdf/rapport_et_communique_de_presse/(2011)/4-La-cooperation-internationale-en-matiere-de-lutte-contre-la-fraude.pdf

Observatoire de la sécurité des cartes de paiement (2011), *Rapport annuel de l'Observatoire de la sécurité des cartes de paiement*, Official report

ORACLE (2011), *Oracle financial services know your customer*, Data sheet

PUGNET Jérôme, KONG Tomas (2014), *Detect faster and prevent better with SAP Fraud management*, Article, SAPinsider

PwC (2014), *Economic Crime Survey* [online]: http://fr.slideshare.net/PwCFrance/pw-c-etudefraude(2014)

SAP (2013), *Detect, prevent, and deter fraud in Big Data environments*, Solution brief

SAS (2012), *SAS® Text Analytics*, Solution overview

SAS (2012), *SAS® Fraud network analysis*, Product brief

SAS (2011), *SAS® Fraud management*, Product brief

Searchdatamanagement (2014), *Definitions*, [online]: http://searchdatamanagement.techtarget.com

STUART Alix (2012) , *Big Data playing a bigger role in fraud-spotting*, Article, Compliance week

The Fraud Management Institute, Bridgeforce (2010), *Protecting the Enterprise: Social Network Analysis - Connecting the Dots*, Research Report, Sponsored by SAS

TURNER Donna, STEWART David (2013), *Effective fraud management*, Conclusions paper SAS

VERSACE Michael (2014) , *The challenge of bank fraud, Interview report*, IDC Financial Insights

APPENDIX

Appendix 1: Document posted on LinkedIn and Slideshare

Appendix 2: Interview guide (Jérôme Pugnet, SAP)

Appendix 3: Interview guide (Chip Kohlweiler, Deloitte)

Appendix 4: Useful definitions

Appendix 5: Banking Related Fraud Schemes

Appendix 1: Document posted on LinkedIn and Slideshare

MASTERS THESIS

PROBLEMATIC: Managing the risk of fraud with Big Data in the banking industry, a consulting perspective

PART 1: Traditional fraud risk management solutions are still the most widely used methods in the banks but they tend to become weak in a context of Big Data expansion
1. Description of traditional methods (still the most widely used methods) and their benefits
2. Limits of the traditional methods in the context of Big Data expansion
3. New methodologies of fraud risk management

PART 2: Big Data as a big opportunity for fraud risk management in the banking industry
1. Big Data solutions seem to be more appropriate nowadays (cover limits of traditional methods, such as including structured and unstructured data)
2. Importance of reliable Big Data tools for an efficient fraud risk management (reducing false positives, more accurately define what risks areas to monitor and speed the processes)
3. Big Data solutions tend to be more beneficial and least costly

PART 3: … But Big Data solutions are not yet usual nor accessible to every bank
1. The cost of implementing Big Data solutions/tools for a fraud issue is still high (cost of transforming big data into information, sophisticated technologies)
2. Challenge of getting full advantage of Big Data (Forensic Data Analytics challenge, qualified personel, Big Data training not yet widespread)
3. Big Data solutions cannot replace traditional methods and finding fraud still relies on human intelligence (asking the right questions, each fraud case is different from the other)

PART 4: What Consulting firms can use from our study
1. How does a consulting firm helps its client to manage fraud risk using big data?
2. What are the biggest challenges for a consulting firm in implementing an FDA solution?
3. The added value of our conclusions for consulting firms (i.e. a conceptual framework, focus on specific areas, argue to sell a big data solution to a client)

Semi-structured interview guide 1
For a Big Data fraud management solution provider

Question 1:
According to you, what are the main limits of banks' traditional fraud management solutions in the context of Big Data expansion?

Question 2:
How does your solution cover these limits?

Question 3:
Can you briefly explain how does your solution work?

Question 4:
To which extent does your solution increase the efficiency of the bank's fraud risk management?

Question 5:
What are the cost and the cost savings (estimated) of your solution for a bank implementing it (from the implementation to the yearly use)?

Question 6:
Is there any other benefit you want to mention?

Question 7:
What are the biggest challenges in implementing your solution?

Question 8:
What does the bank need in addition to your solution to get full advantage of it (qualified personnel for example)?

Question 9:
How does your solution differ from other comparable solutions on the market?

Question 10:
How do you sell your solution to a client? What are your main arguments?

Question 11:
What are the limits of your fraud management solution?

Question 12:
Is there something we definitely can't drop out from the traditional methods? If so, what?

Question 13:
According to you, what are the key success factors of a fraud management solution in a context of Big Data expansion?

Semi-structured interview guide 2
For a Big Data fraud management solution user

Question 1:
What were the main limits of your previous fraud management solution? Why did you decide to go for a Big Data solution?

Question 2:
How and why did you choose the solution you implemented?
How does it cover the limits of your previous solution?

Question 3:
Can you briefly explain how does the solution work?

Question 4:
Did it increase the efficiency of your fraud risk management? If so, how?

Question 5:
What has been the cost of the initial investment and what is the cost of the yearly use? Did you achieve cost savings? How?

Question 6:
Is there any other benefit you want to mention?

Question 7:
What have been the biggest challenges in implementing and using the solution?

Question 8:
What did your company need in addition to the solution to get full advantage of it (qualified personnel…)?

Question 9:
What are the limits of your current fraud management solution?

Question 10:
Is there something you definitely can’t drop out from the traditional methods?

Question 11:
According to you, what are the key success factors of a fraud management solution in a context of Big Data expansion?

Semi-structured interview guide 3
For a Consultant

Question 1:
What are the main limits of your clients’ fraud management solutions? Has this something to do with modern fraud risks due to Big Data expansion?

Question 2:
What are you advice? Do you advise Big Data solutions (advanced analytics…)?

Question 3:
Can you briefly explain how do the solutions work?

Question 4:
Did it increase the efficiency of your clients’ fraud risk management? If so, how?

Question 5:
What is the cost of the solution (investment, yearly use…)?
Did your clients achieve cost savings? How?

Question 6:
Is there any other benefit of the advised solutions you want to mention?

Question 7:
What have been the biggest challenges in implementing and using the solutions for your clients?

Question 8:
What did your clients need in addition to the solutions to get full advantage of it (qualified personnel…)?

Question 9:
What are the limits of the advised solutions?

Question 10:
According to you, is there something you definitely can't drop out from the traditional methods?

Question 11: According to you, what are the key success factors of a fraud management solution in a context of Big Data expansion?

Appendix 2: Interview guide (Jérôme Pugnet, SAP)

Question 1:
According to you, what are the main limits of companies' fraud management solutions in a context of Big Data expansion?

Question 2:
How does the SAP Fraud management solution cover these limits?

Question 3:
Can you briefly explain how does the solution work? What are the key features?

Question 4:
To which extent does SAP Fraud management increase the efficiency of the company's fraud risk management? (Accuracy, false positives, time, prevention…)

Question 5:
Is there any other key benefit of the SAP fraud management solution you want to mention?

Question 6:
What are the biggest challenges in implementing SAP fraud management?

Question 7:
Is it possible to implement / integrate SAP fraud management on the existing IT infrastructure if it's not SAP? (ERP system from a competitor for example)

Question 8:
Does the company need a team of experts such as data scientists to get full advantage of the solution?

Question 9:
What does the company need in addition to SAP Fraud management to get full advantage of it? For example: talk with IT to explain what data the fraud team need.

Question 10:
How would you sell SAP Fraud management to a bank? What would be your main arguments?

Question 11:
If any, what are the limits of the SAP Fraud management solution?

Question 12:
According to you, is there something you definitely can't drop out from the traditional methods?

Question 13:
Do you have advice for consulting firms helping their clients to manage fraud risk?

Question 14:
According to you, what would be a good framework for managing the risk of fraud?
What do you think about this 6-phases process:

1) Assess risk
2) Define objectives
3) Obtain data
4) Develop and apply procedures
5) Analyse results
6) Manage results

Question 15:
Is there any whitepaper, case study or client's presentation relative to the topic you want to share?

Appendix 3: Interview guide (Chip Kohlweiler, Deloitte)

Question 1:
According to you, what are the main limits of banks' traditional fraud management solutions in the context of Big Data expansion?

Question 2:
What are your advice to cover these limits?

Question 3:
What kind of solutions do you advise? Do they leverage Big Data to manage fraud? What are their key features?

Question 4:
To which extent do the solutions you advise increase the efficiency of the bank's fraud risk management? (Accuracy, false positives, prevention, flexibility to adapt to the new fraud schemes…)

Question 5:
What do banks take into account when deciding to implement a Big Data solution? (ROI…)

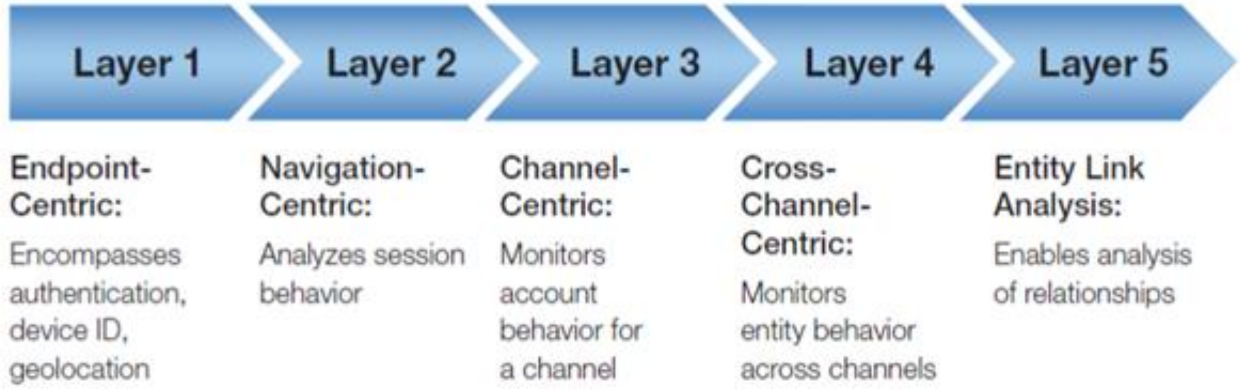
Question 6:
What are the biggest challenges in implementing the solutions you advise?

Question 7:
Does the bank need a team of expert such as data scientists to get full advantage of the solution? (Predictive analytics…)

Question 8:
What are the limits of the fraud management solutions you advise? What about data privacy?

Question 9:
Is there something we definitely can't drop out from the traditional methods? If so, what?

Question 10:
According to you, what would be a good framework for managing the risk of fraud today? What do you think about the "layered approach for fraud prevention" developed by Gartner:


Layer 1
Layer 2
Layer 3
Layer 4
Layer 5
Endpoint-Centric:
Encompasses authentication, device ID, geolocation
Navigation-Centric:
Analyzes session behavior
Channel-Centric:
Monitors account behavior for a channel
Cross-Channel-Centric:
Monitors entity behavior across channels
Entity Link Analysis:
Enables analysis of relationships

Question 11:
To sum up, what are the key success factors of a fraud management solution in a context of Big Data expansion?

Appendix 4: Useful definitions

Ad hoc data analytics: one-use process, a starting point that may be used to help identify patterns or potential risk areas within a business system. (ISACA)

Big Data: term used to describe large collection of data (from traditional and digital sources inside and outside a company) that includes structured and unstructured data, and grows so large and quickly that it is difficult to manage with traditional processes or tools. It is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making (Gartner, Inc.)

Continuous monitoring data analytics: At this stage, analytics are fully automated and running at regularly scheduled intervals and may be embedded directly into a production system. A continuous run of analytics enables the immediate identification of potential exception transactions. The benefits to the enterprise include improved efficiency, reduced errors and timely identification of problems.

Data analytics: involves processes and activities designed to obtain and evaluate data to extract useful information. Evolution of Data analytics techniques: Ad hoc, repeatable, centralized, continuous monitoring. (ISACA)

Due diligence: investigation of a business or person prior to signing a contract, or an act with a certain standard of care.

Data mining: analysis of large data sets by a computer program to identify patterns (business rules) that exist within the data. (ISACA)

Forensic Data Analytics: seek out indicators of fraud in the data. Ability to collect and use data both structured and unstructured to identify areas of potential fraud or corruption. FDA can also include integrating continuous monitoring tools, analyzing data in real-, or near-real, time and enable rapid response to prevent suspicious or fraudulent transactions (E&Y 2014 *Big risks requires Big data thinking*)

Hadoop: framework that allows for the distributed processing of large data sets across clusters of computers using simple programming models. It is designed to scale up from single servers to thousands of machines, each offering local computation and storage (from The Apache Software Foundation). Another definition: foundational framework of Big Data that uses distributed processing of massive data streams of unstructured and structured data sets across clusters of computers using simple programming models

Know your customer (KYC): policies mandated by regulators globally to prevent fraud and money laundering.

Predictive: Estimate a future event on the basis of knowledge and reasoning

Predictive data analytics: analysis of large data sets for the purpose of predicting future activity patterns based on past transactions. (ISACA)

Predictive modeling: uncovering patterns to help companies make business predictions such as forecasting where there may be a propensity for fraud

Preventive: acting as an obstacle to

Proactive: Acting in advance to deal with an expected change or difficulty

Proof of concept: verify that some concept has the potential of being feasible and used

Semi-structured data: refers to a type of structured data that lacks the strict data model structure. For example, emails have the sender, recipient, date and other fixed field added to the unstructured data of the email message content and attachments.

Social Network Analysis: developing a complete picture of any fraud event by finding specific entities (individuals, accounts and transactions) that may be involved in fraud and then establishing links between these suspect entities and other entities that may be related. Once the links are constructed, they need to be refined with analytical techniques to produce meaningful networks that have a high likelihood of actual or potential fraud (The Fraud Management Institute, *Protecting the Enterprise: Social Network Analysis - Connecting the Dots*)

Structured data: refers to data that resides in a fixed field within a record or file (row-column database).

Text analytics: involves the structuring of text from unstructured sources using techniques for parsing words or phrases, and for detecting patterns and connections in the text.

Three "V": often used to describe Big Data, "volume" (the amount of data), "velocity" (the speed of information generated and flowing into the enterprise) and "variety" (the kind of data available). Sometimes there are a fourth and fifth "V": "veracity" and "value".

Unstructured data: refers to data that can't fit neatly in a database (e-mail message, word documents, videos, photos, audio files, webpages…).

Whistleblowing: disclosure by a person, usually an employee in a government agency or private enterprise, to the public or to those in authority, of mismanagement, corruption, illegality, or some other wrongdoing.

Appendix 5: Banking Related Fraud Schemes

Here are a few typical fraud schemes encountered in banking and some examples of the way data analysis can be applied to detect and prevent them:

Corruption

- Find customers who appear on the US Treasury Department Office of Foreign Asset Control (OFAC) list.
- Ensure Financial Action Taskforce on Money Laundering (FATF) compliance.
- Produce listing of transactions with organizations on the list of non-cooperative countries and territories.

Cash

- Identify cash transactions just below regulatory reporting thresholds.
- Identify a series of cash disbursements by customer number that together exceed regulatory reporting thresholds.
- Identify statistically unusual numbers of cash transfers by customer or by bank account.

Billing

- Identify unusually large number of waived fees by branch or by employee.

Check Tampering

- Identify missing, duplicate, void, or out of sequence check numbers.
- Identify checks paid that do not match checks issued, by bank, by check.
- Locate check forgery or falsification of loan applications.

Skimming

- Highlight very short time deposit and withdrawal on the same account.
- Find indicators of kiting checks.
- Highlight duplication of credit card transactions and skimming.

Larceny

- Identify customer account takeover.
- Identify co-opted customer account information.
- Locate number of loans by customer or bank employee without repayments.
- Find loan amounts greater than the value of specified item or collateral.
- Highlight sudden activity in dormant customer accounts – identify who is processing transactions against these accounts.
- Isolate mortgage fraud schemes – identify “straw buyer” scheme indicators.

Financial Statement Fraud

- Monitor dormant and suspense General Ledger accounts.
- Identify Journal Entries at suspicious times.