ovum

Assessing the role of Big Data in tackling financial crime and compliance management

Examining real use cases and its potential

Summary

Catalyst

The banking industry paid over $65bn in regulatory penalties in 2014, with misconduct and anti-financial crime failures core indictment grounds. Unsurprisingly, tackling financial crime and compliance management have become top of mind executive issues; a position set to continue given the ongoing intensity of regulatory demands. However, many banks are finding that existing processes and infrastructure are struggling to effectively support evolving requirements, resulting in significant growth of associated operational costs. In this context, recent developments in data analytics, which allow faster analysis of larger, more complete, and more varied data sets, appear to have the potential to solve some of the major pain points. This paper looks at the evolution of Big Data in this space, examining use cases where advanced analytics is already being deployed, and its longer-term potential.

Ovum view

Hadoop will become a vital data platform in the banking sector for tackling financial crime and compliance. Banking institutions will no longer be restricted to analyzing data samples. The ability to deal with higher volumes of data, and work with new, unstructured data types will significantly enhance the analysis of suspicious activity, providing more complete detection and driving lower false positives. This will be vital for banks needing to tackle the conflicting pressures of managing compliance breaches, while controlling operational costs and minimizing customer inconvenience. The platform has already matured to the point to where it is now being used in live deployment, such as to improve digital banking security or manage regulatory reporting. With most banks actively working with this technology, Ovum expects significant adoption over the next 2-3 years.

Key messages

- Ongoing policy changes and new requirements are challenging previous approaches to compliance management
- Advanced analytics is providing new ways of working with data, and incorporating insight into the business
- Institutions are now able to work with the full dataset in analyzing potential financial crime, allowing them to get the complete picture on potentially noteworthy incidents or trends that are more reliable than traditional approaches relying on samples
- Ability to work across multiple data types, such as voice, chat, email, and machine logs, will be key for tackling insider misconduct risks
- Institutions have already started to use Big Data in supporting live financial crime and compliance management functions

Key recommendations

With the shift in the regulation towards a risk-based approach continuing, institutions need to look to adopt best-practice in tackling financial crime and managing compliance. With a number of banks now taking advantage of the Hadoop platform, this means institutions have both a regulatory and business imperative to look to incorporate Big Data in their compliance functions.

Compliance demands are challenging established approaches to data and analytics

Ongoing policy changes and new requirements are challenging previous approaches to compliance management

Western banks were subject to over $65bn in regulatory penalties in 2014, a 40% raise on the 2013 level. While perhaps a high water mark in terms of total fines, regulators have made it clear that they are expecting a sea change in the sector's conduct, with limited tolerance for further compliance management failures. Alongside this stricter enforcement, associated requirements remain steadily increasing in terms of both intensity and reach, with financial institutions expected to take a proactive and risk-based, rather than checklist or merely procedural, approach to compliance.

At an execution level, this is ultimately a people issue, with regulators looking to change the industry's culture and approach to compliance. However, it is resulting in significant growth of operational overheads as institutions have to expand supporting business functions and technology capabilities, to improve the effectiveness of processes and to drive compliance-led decision making throughout the institution.

AML, CTF and sanctions requirements shifting towards risk-based approaches and outcome-based responsibilities

Anti-financial crime responsibilities are long-standing ones for the financial industry. Coordinated inter-government policy standards date back to 1990, with the first Financial Action Task Force (FATF) report to address money laundering, and country-specific requirements in most mature markets dating significantly before that. Indeed for the US, the Bank Secrecy Act (1970) and Money Laundering Control Act (1986) remain key pieces of legislation.

While the general responsibility is a longstanding one, actual demands have broadened significantly in recent decades; a trend set to continue rather than abate. The 1980s and 1990s saw policy driven by anti-money laundering (AML), particularly related to drugs and organized crime-related activities. This extended in the 2000s to counter terrorist financing (CTF), with the USA PATRIOT ACT in 2001 of high significance here. (The primary difference here is that 'clean' money is flowing to fund unlawful activity, rather than trying to make 'dirty' money from unlawful activity become 'clean'.) In more recent times, regulatory attention has seen reinforced scrutiny on ensuring adherence to financial and trade sanctions, with BNP Paribas' record $8.9bn penalty in 2014 for violations of US sanctions on Iran clearly illustrating current tolerance levels.

Such directives are continuing to widen, with banks expected to take an increasing role in preventing financial activity related to bribery and/or corruption. Likewise tax evasion responsibilities are likely to be dominant in the next wave of regulatory attention, such as with the US's FACTA requirements demanding non-US banks report on US citizens.

In additional to this increased breadth, demands have also steadily intensified. Requirements have extended over each policy cycle to broaden the scope of applicability (e.g., remit is widened to cover more institution types), while becoming both more detailed and prescriptive (i.e., more mandatory elements). For example, the Fourth Money Laundering Directive (MLD4), published in June 2015, adds new provisions around dealing with political exposed people (PEPs); explicitly including tax crimes; and clarifying and reinforcing rules on Customer Due Diligence.

While this intensity and breadth will continue to grow, recent requirements (such as seen with MLD3, and taken further with MLD4) have also shifted implementation focus towards a risk- over rule-based approach to tackling financial crime. This is a key change. While institutions get more leeway in decision-making in some areas (for example they don't have to automatically drop risky clients), it means that compliance or money laundering officers don't have the default position of deferring to the 'rulebook' when implementing policies. Rather, firms need to identify, understand, offset and document any risks, while ultimately being accountable for any decisions they make. Crucially, it means that actual outcomes are more important than whether an institution has adhered to specific rules (although these remain critical as well). Compliance thus becomes less a back-office, checkbox-led supervisory function, but rather a core part of day-to-day operational processes and decision-making.

While there are differences in this risk versus rules balance approach at a country level, this shift towards an outcome-based regulatory approach is becoming the norm. This is both for financial crime and for compliance management in general, be it around consumer protection (such as UDAAP in the US or TCF in the UK) or wider conduct risk issues, to prevent behavior such as seen with the Libor rate-fixing scandal.

Requirements necessitate technology platforms enabling controls and robust management reporting

Specifications for putting requirements into practice level are now extensive and would fill several papers. However, key components of an effective risk-based compliance program now include:

- An effective governance framework that demonstrates strong board/executive backing for a culture of compliance, reinforced across strategy, performance review and compensation processes
- Well-defined (and sufficiently resourced) compliance roles and responsibilities which provide delineated layers of defense for credible and effective challenge
- Clear and well-communicated strategy and policies, which are understood appropriately across the institution through customized training
- Risk assessments that identify and develop appropriate controls to manage risk at multiple levels, including enterprise; line of business (LoB) and/or legal entity; horizontal (e.g., across LoBs); product/service; geography; customer; and compliance type (e.g., sanctions, AML, or conduct)
- Robust management reporting that includes necessary metrics to measure and monitor risks and performance
- Ongoing monitoring and periodic independent review of program effectiveness itself

While many of these requirements are people, policy, and process related, technology systems are a core enabler of effective compliance management. This is within the compliance function itself, with case management and analytics platforms assisting operations staff with workload prioritization and managing caseload volumes/quality. It is also in broader compliance program implementation, particularly in development of 'appropriate controls'. These include systems that enforce policies (e.g., prevent transactions that fall outside of risk-defined policies), mandate information-gathering requirements (e.g., during origination processes), or provide automated monitoring and analytics to detect potentially suspicious activity. Further systems are essential in the creation of 'robust management reporting', allowing risk/performance metrics to be measured and monitored, at both an aggregated and granular level; up to date, through automated data collation/processing; accessible,

such as through dynamic, business intelligence tools; as well as traceable, providing ability to track underlying supporting data and preparation workings.

Importantly, a central demand from regulators is to ensure that controls and reporting systems actually drive business decision-making, as opposed to merely driving high volumes of regulatory reports. This is both at the senior management level, so that identified risks, flags and actual incidents are in fact responded to, and at an operational-level so that compliance-led insight is embedded into day-to-day operations and decision-making.

The requirement for ongoing monitoring and periodic review of program effectiveness itself means that creation of the supporting technology platforms is not a one-off exercise. Alongside the shift to a risk-based approach, the onus is on institutions to ensure they are adopting best practices in managing compliance and financial crime risk. This is performed at business function level, with institutions needing to ensure that they maintain awareness of latest risks and requirements, and at the technology level, to ensure techniques and controls maximize effectiveness.

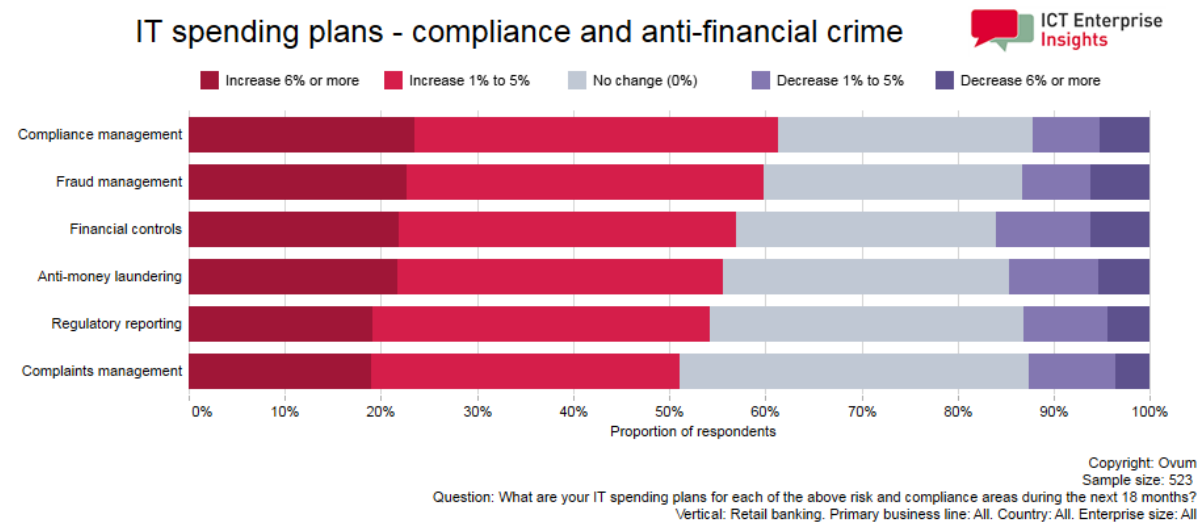
Increasingly, getting a clear picture of risk requires incorporating non-traditional data sources to improve the efficiency of detection and due diligence techniques; this may be especially true for higher-risk customers that require enhanced analysis. This involves moving beyond the traditional internal banking transaction datasets (that form the core of most existing approaches) to include new and evolving data sets, such as machine log data, clickstream data, social media, documents, newsfeeds, images, and video that may be derived externally as well as from within an institution. These can allow institutions to detect new potential unidentified risks as well enhance effectiveness of detecting and assessing identified risks.

Operational costs are soaring, putting pressure on traditional piecemeal approaches

The impact of increasing compliance demands has been significant. Direct costs have escalated with institutions required to considerably expand staff numbers to support compliance and anti-financial crime functions. Indirect costs have also been notable, such as around employee training, as well as additional time spend by general staff on compliance-related activities. HSBC is a good example here: reporting in 2014 that risk and compliance staff numbers had reached 24,300, nearly 10% of its entire workforce. This had grown by a sixth on three years earlier, and was identified as a prime driver in the growth in its underlying operating expenses (with most other functions conversely reducing costs).This trend was expected to continue in 2015. Although, as a global systemically important bank HSBC was already receiving close regulatory scrutiny, the bank has been far from alone is this respect, with most reporting similar pressures

Significant investment has also been made in compliance-related technology infrastructure, which is expected to continue. According to Ovum's ICT Enterprise Insights program (a global primary research study conducted in Q3 2015 with senior IT executives on IT spending plans), over half of the 500+ banks interviewed plan to further increase expenditure across the main compliance and anti-financial crime areas in 2016 (see Figure 1). Indeed, around a fifth are still expecting to require significant (i.e., over 6% spend) growth here. This is despite the fact that spending on compliance has already grown significantly since the financial crisis.

Figure 1: Banking IT spend growth plans across compliance and anti-financial crime activities



Source: Ovum ICT Enterprise Insights 2015/16

For many banks, such mandatory-driven spend now constitutes a significant proportion of available change-the-bank investment within IT budgets. As a result, effectively managing growing compliance costs is now a major business imperative. This is driving a shift from tackling compliance requirements on piecemeal basis (i.e., dealing with each regulation as a separate project) towards taking a platform approach. Many of these demands have significant commonalities across data sources, collation and preparation, analysis, and reporting needs; therefore, banks need to search for approaches that allow infrastructure to be leveraged across current, and for future, requirements.

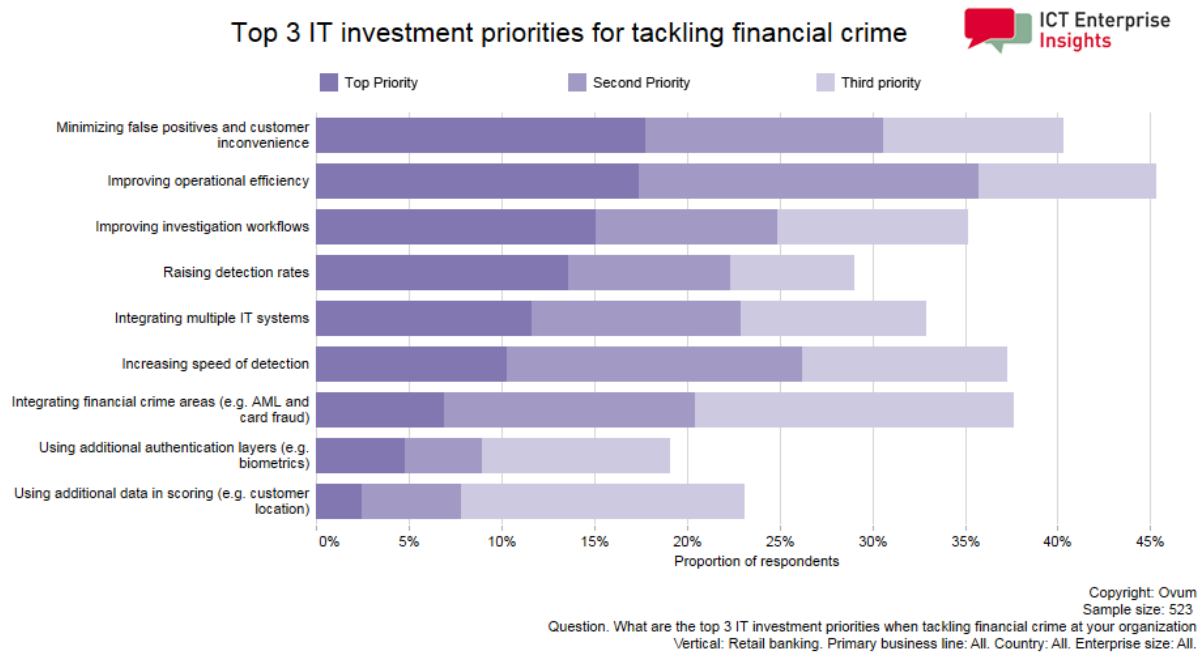
New requirements for improving effectiveness and speed of detection to streamline anti-financial crime activities

This is resulting in three key imperatives for compliance and anti-financial crime divisions:

- The need to improve the effectiveness of controls and detection techniques, enhancing both discovery levels and speed of discovery to meet regulatory requirements
- The need to manage the cost of supporting operations, to drive operational efficiency and increase productivity of operations staff
- The need to minimize the negative impact of such activity on customers, such as through false positives, resulting in refusal or delay to customers in conducting their financial activity

The impact of these on IT priorities is illustrated in Figure 2. This also shows data from Ovum's Enterprise Insights program, detailing top IT investment priorities for the banking sector in tackling financial crime for 2016.

Figure 2: Top IT investment priorities for tackling financial crime



Source: Ovum ICT Enterprise Insights 2015/16

Minimizing customer inconvenience is a key priority, closely followed by desire to improve operational efficiency, with increasing detection rates and detection speed also identified as important. Reflecting the pressure to adopt best practice, the need to use additional data is also emerging as a significant third priority. However, in many respects these areas are heavily linked, with analytic capability at the core; the ability to rapidly -- and importantly correctly -- identify illegitimate activity is beneficial for regulators, customers, and efficiency. Reducing false positives not only reduces customer inconvenience, but also reduces the workload of supporting operations functions.

Conventional data warehouse and business intelligence techniques are struggling to support flexibility, speed and cost demands

Banks are already well-versed in traditional SQL-based analytic techniques, given longstanding information requirements across risk, compliance, finance, and business functions. Here, data from source systems is extracted, transformed, and loaded (ETL) into an analytical SQL database based on specified schema; this is typically either a specific data mart or a more general data warehouse. Queries are then run on this processed data to conduct analysis, generate reports, or create models to drive operation decision-making. Historically, this was managed within the realm of the specialist analyst, although development of business intelligence tools, such as dashboards or visualization engines, have allowed the resulting information to be more accessible across the business through self-service and interactive portals.

This approach is effective in many situations, particularly when dealing with structured data, such as what is found in most banking source systems (which tend to be transaction-centric). It generally provides a high degree of resulting analytic output accuracy and reliability, which of course is an important requirement for risk, compliance and finance functions. And it will remain the core to many processes targeting risk, fraud prevention, and compliance.

However, SQL data warehousing is not without challenges. These systems are not designed to handle variably structured data, an area where most institutions are seeing substantial volume growth as client interaction and business processes become more digitalized. This includes:

- Machine-generated data sources, such as log files from online/mobile interactions, telephone call detail records (CDRs), or network events;
- Social and internet data (e.g., from Twitter, Facebook or Google); and
- Less structured data within an institution, such as contracts, emails, documents, voice, photos, and videos.

These alternative data sources represent a wealth of new data to mine; however, SQL approaches that require pre-set schema are poorly suited for handling these data types because the schema are varying, and in many cases, constantly changing. It would become practically impossible for static ETL processes to keep pace with the highly dynamic, variably structured data sources that are now becoming critical for piecing together a comprehensive picture of risk . In practice, it means that, traditionally, most analysis was only conducted on a small proportion of such data sources.

Even with structured data sources, there is a significant cost overhead in maintaining the ETL layer between source and analytical database systems to ensure data currency and quality. This can be manageable if data sources are all known upfront and have unchanging structures, but it can be a major challenge to accommodate new data sources and inflexible when dealing with rapid change.

Alongside this, data warehouses have relatively high storage costs, which are compounded by high ETL costs and long refresh times for large data sets. Not surprisingly, most institutions traditionally conducted analysis on a subset of more recent and deemed relevant data. For example, analysis would have been performed on applicable transactions over the past year, rather than all possible data collected over the last ten years. And they wouldn't factor related data, such as email, call center records, or social data that could add important context. For predetermined questions this might be acceptable, as appropriate data can be identified and significance prioritized; however, it is suboptimal for exploratory analysis (such as identifying emerging fraud trends) and means that analysis is not really complete. Data visibility (e.g., ability to drill-down into lower levels) is also often lost in due to these factors, with aggregated processed data used to reduce processing time for querying large data sets, with underlying raw data often removed.

Processing scalability also tends to be non-linear with higher volumes of data or more complex analytics resulting in extended batch processing run times. This means that analytics users typically have to make a trade-off with the traditional SQL approach between richness and reach. Rich, complex analytics can be conducted if data size is limited (or run with a long batch window), or conversely analytics can be conducted more rapidly with larger data sets if problems are kept simpler.

Big Data analytics providing new paths for addressing fraud and compliance issues

New ways of working with data, and incorporating insight into the business

The analytics world has experienced a revolution over the last half-decade, prompted by the explosion of data across the Internet-connected world and from machine-generated sources, which has required

new techniques to supplement or replace SQL-based query and analytics. Often referred to under the tag of ‘Big Data’, new approaches extend the range of data types that can be covered and provide alternative techniques for storing and analyzing data, such as through programmatic approaches utilizing languages such as Java, Python, or R. These can cost-effectively extend the scope of analytics to include all, not just a sampling, of data, and can drive new and enhanced insights based on a more complete picture. More recent developments, such as around the Spark computing engine, have seen the capability to bring real-time analytics, which has important implications in how institutions can operationalize insight.

Perhaps more importantly, this period has also seen a maturing of advanced analytics techniques for use within the enterprise. Implementation ease and manageability have improved, with institutions able to combine new programmatic and SQL approaches (with latter also evolving in response). And, significantly for banks, data governance best practices for audit and control purposes have caught up to meet enterprise and regulatory requirements. While still a rapidly evolving area, it is one that is becoming enterprise-ready, allowing it to be applied to real business challenges.

Data lakes offer more complete approaches to for data storage and utilization

Newer techniques take a fundamentally different approach to storing and working with data. The ‘data lake’ concept is a good example here, with Hadoop as the best known platform for supporting this use case. The data lake is an implementation pattern that is suited for organizations that have already gained experience working with the Hadoop platform, understanding of how to work with big data, and building expertise regarding what data should be retained.

In a data lake, data is loaded into the platform in its raw form, stored through a highly scalable, open source distributed file system across large clusters of commodity servers, and with the ability to perform massively-parallel computation (again using commodity computing power) and support multiple access methods (e.g., batch, real-time, in-memory, streaming) and multiple workloads. This offers a number of advantages:

- Significantly lower cost of processing and storage – The ability to leverage commodity servers and direct attached commodity high-capacity drives results in a cost of storage several magnitudes lower that with high-end Storage Area Networks or Massively Parallel Processing architectures used in most data warehouses.
- Ability to store all data – Lower cost and massive scalability means that this is practically feasible, and so raw data as well as any processed or aggregated data can be maintained. This simplifies data lineage discussions (whereas raw data is not always maintained with SQL approach), and provides maximum flexibility for future analytics.
- Ability to store all types of data – Data does not need to be structured until it is analyzed or queried.
- Flexibility to store new data – Because storage is not bound by any pre-set schema.
- Creation of a common data set – With the ability to store all data and perform multiple workloads means that data does not need to be fragmented and maintained in siloes to meet needs of different users across the institution. Instead, the platform can act as a shared resource, containing centralized versions of the data.

The end result is a new approach to analysis. Rather than a linear approach where data is collated in response to specific questions, and then refined if additional questions are detected/required, the

ability to conduct analysis across all data enables organizations to conduct exploratory analytics to identify data, patterns, and queries to pursue. In effect, the data can drive the questions being asked, allowing institutions to pick up on relationships, trends, and patterns than may have not otherwise be identified. It allows financial institutions to think outside the box as they identify and analyze unanticipated patterns of risk.

Real-time analytics can be incorporated inline into business processes

The advantage of this approach is that it starts to allow a more joined-up approach between business analytics and the operational processes that this supports – where analytics becomes embedded in the operational process.

Leveraging a common platform

Hadoop is no longer just a MapReduce batch processing machine. The current second generation of the platform was designed to logically divide clusters to allow multiple workloads to run concurrently, so batch, interactive, and real-time workloads can work side by side. For instance, an institution could use the analytics to react to transactions as they occur, with compliance/fraud operations teams performing interactive processing during the day alongside batch-oriented to perform more exploratory analysis. The same cluster could then run a series of batch modeling processes overnight. In this situation, incorporating new insight obtained is a more straightforward process, whereas with the traditional data warehouse and operational application approach, the 'closed loop' between systems, if there is one, is often protracted.

Spark's emergence

A key recent development in the Hadoop ecosystem in this respect has been progression of the Spark compute engine, which brings real-time analytics and flexibility to the platform. This is a new distributed processing engine that provides several distinct advantages:

- It takes advantage of in-memory processing to support real-time analytics and make iterative, machine learning practical;
- It provides a modular engine with common APIs that can support a wide range of analytic approaches, including (but not limited to) streaming, machine learning, graph processing, and SQL. And these analytic approaches can be orchestrated, so for instance, machine learning could be employed in conjunction with analysis of real-time streaming events.
- It provides access to an expanding group of third party libraries for performing analytics.

Evolving data governance and user tools area targeting data lineage and usability

While the data lake approach with Hadoop does offer many advantages, it is not without issues. Development of the Hadoop ecosystem was originally driven primarily by Internet-based companies, with likes of Google, Yahoo, Facebook catalyzing (or indeed performing) much of the initial development. With significant IT and engineering skillsets most of original focus was on capability rather than usability, manageability, or security; the emphasis was on performing highly data-intensive analytics of log files for optimizing search indexes or ad placement. This required sophisticated skills for writing MapReduce programs. Furthermore, as a platform only known by a few experts, performing analytics on relatively non-sensitive data, practices such as managing security, access, privacy, and audit obligations were of little concern.

However, as Big Data has moved into the mainstream enterprise world over the last half-decade, these concerns have grown paramount, especially for regulated industries like banking. Tools and

capabilities, both open source and proprietary, are becoming available to regulate access, selectively mask or encrypt data, orchestrate data transformation operations, and track lineage. They are providing the building blocks for banking institutions to implement data lakes that are governed to support privacy (e.g., managing protection of sensitive items of data, such as accounts numbers, to ensure they are automatically masked) to support internal policies and satisfy regulatory mandates.

Additionally, while the SQL and classic MapReduce-style programmatic analytics emerged from different worlds, they have converged over the last five years, with Hadoop able to work alongside the data warehouse. There are new access paths where SQL queries to relational databases can be processed in Hadoop, while the results of MapReduce or Spark analytics can be populated to data warehouses for further query. For instance, Oracle Big Data SQL allows queries to be submitted from the Oracle database, with the processing pushed down into Hadoop, where the data is surfaced as virtual Oracle tables. Additionally, use of techniques such as Spark Streaming can perform basic analysis of trends in real-time events in Hadoop, with the results populating data sets that can then be fed into the Oracle database using the Oracle Loader for Hadoop. Both approaches allow organizations to gain the best of both worlds: the familiar query and analytic environments of data warehouses with the unique processing capabilities and inexpensive, scalable storage on Hadoop.

How Big Data techniques are transforming financial crime and compliance management

Financial institutions are already benefiting from Big Data

The adoption maturity of Big Data in banking has shifted significantly over the last five years, moving from a 'trend to watch' at start of the decade, to experimentation, and then piloting in more recent years. It has now being deployed in live operation in a number of banks. While still at early stages in moving towards full potential, benefits are being seen in actual use cases.

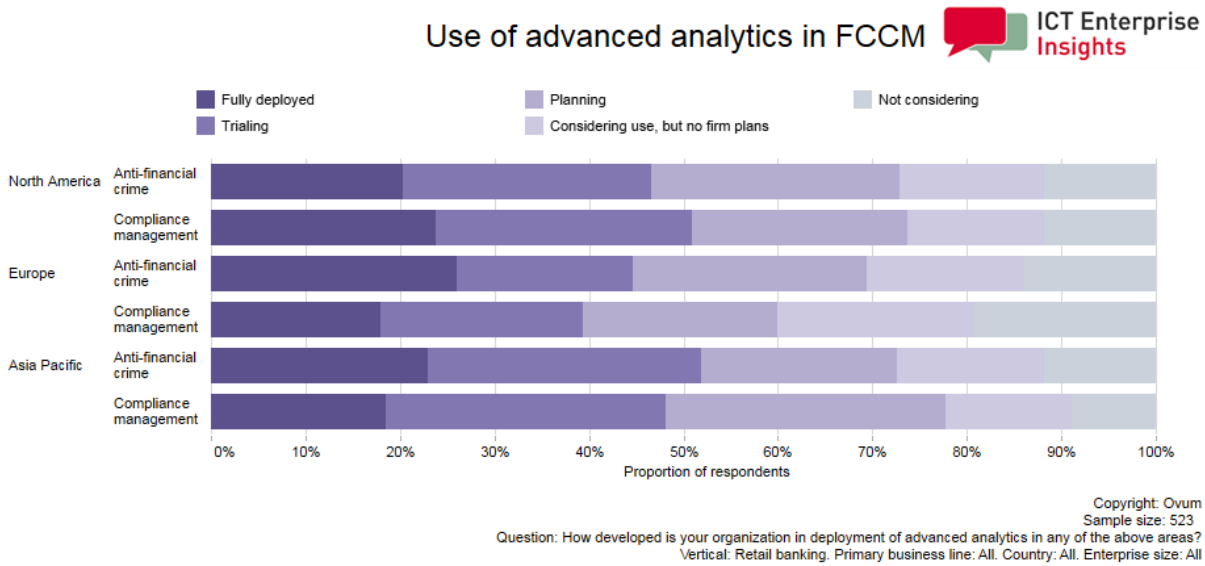
Within the financial crime and compliance management space, key examples here include:

- Use of web session data to enhance online banking anti-fraud and cyber security;
- Creation of data lakes to provide a data foundation layer to meet ongoing regulatory requests; and
- Ability to run fraud analysis across the whole credit card transaction set to improve completeness.

Use of advanced analytics by banks within financial crime and compliance is starting to become mainstream

Given the rapid advances in analytics over the last five years, the maturity of adoption within the banking sector is still nascent. However, it has progressed quickly, and most banks are in serious evaluation or planning stages to incorporate this technology. Figure three highlights this, with data from Ovum's ICT Enterprise Insights program finding strong interest in advanced analytics on both anti-financial crime, and compliance management sides.

Figure 3: Maturity of advanced analytics adoption in FCCM by region



Source: Ovum ICT Enterprise Insights 2015/16

Globally, around a fifth of banks already have some investment in production; this is led by the larger US banks, although activity is common across the three main regions. Another 50% of banks are actively interested, split evenly between institutions in the more advanced, trial stage and those actively planning. Overall consideration is high, with only 10-15% of banks across regions, and across financial crime and compliance, not interested in looking at advanced analytics. This is a reflection of its potential in this area, but also of course regulatory pressures to adopt best practice in these areas.

Enhancing Fraud and cyber-security using new data sources

An example of Big Data analysis in production at a number of banks is the use of new data sources to improve fraud detection and cyber-security, particularly with respect to online banking. Here web session data is being used to create a profile of a user's typical activity patterns. This is used alongside with other anti-fraud approaches (e.g., whether the payee for the new payment instruction falls with previous patterns) to help identify actions that that maybe result of fraudulent access, with the bank able to impose additional security validation check in this case.

This approach uses machine-generated log data and message transmission from the web sessions, (i.e., clickstream data) to understand the paths users take when using websites. This data contains variably structured elements, such as user and page request details, and is very difficult to analyze with SQL methods given the significant preparatory work required to link the data together. In contrast, path analysis is relatively straightforward running the Spark compute engine on Hadoop, and importantly can be done on a real-time basis to allow deployment while activity is being conducted. This means institutions can implement measures to prevent fraud losses rather than need to react post-event.

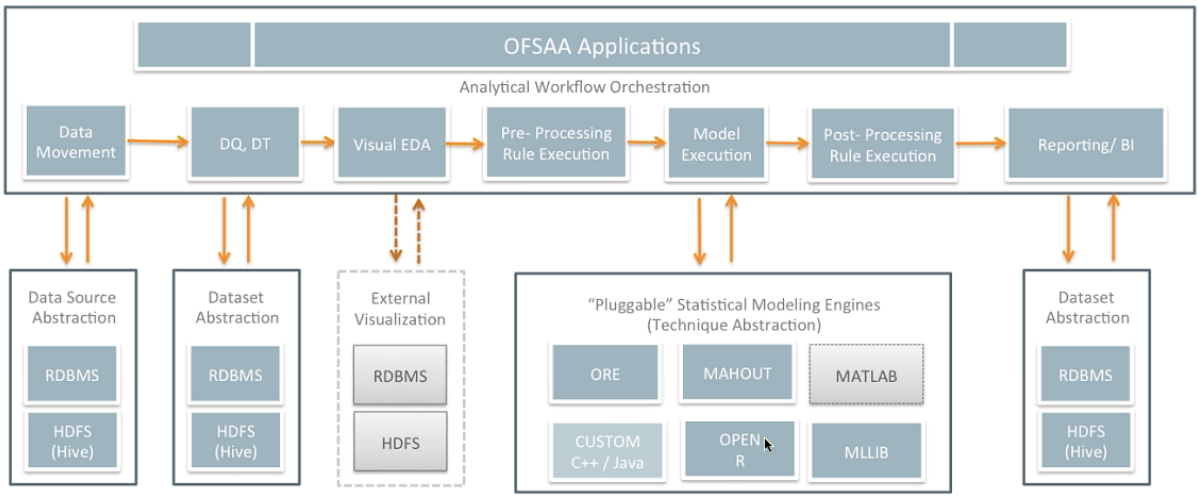
Data lake approach is allowing institutions to rapidly respond to regulator demands

A top-tier US bank institution has used the data lake concept to create a data platform for managing regulatory information requests, particularly relating to dealing with regulatory Matters Requiring Attention (MRA) demands. Previous to this approach, such requests were dealt with on an ad hoc basis, (i.e., as received) with relevant data identified, extracted, analyzed, and reported for each

demand. However, the significant growth in volume made the task more time consuming and costly, particularly given regulatory requirements to show data lineage, provide granularity, and ensure that the data was consistent across each request.

Using a data lake approach, the institution has created a central data-as-a-service platform that can store all relevant data using Hadoop (along with SQL), along with an analytical workflow orchestration layer that manages data quality, processing, model execution and reporting. Figure four provide an illustration of the solution architecture (which is based on Oracle's Financial Services Analytics Application infrastructure in this case).

Figure 4: Solution Architecture using Oracle Financial Services Analytical Applications Infrastructure



Source: Oracle

The advantage of this is that supporting information requests to deal with MRA is a far quicker, lower cost, and more controlled process, with the institution able to provide business intelligence-style reporting to the regulator, while easily accessing questions around data lineage and modeling.

Working with full datasets in analyzing potential credit card fraud

Enhancing credit card fraud detection is another area where use of Hadoop has allowed for improved analytical effectiveness. Most banks run real-time basic checks on transactions based on predefined rules and then run batch analysis using more sophisticated models overnight. Given high credit card volumes in top-tier banks, the need to manage batch processing times (which can be lengthy) and cost mean that these models will focus only on certain transactions (e.g., high value) and/or use a sampling of data over time to detect trends. The challenge is that, from a statistical modeling viewpoint, fraud is a rare event detection issue (i.e., number of fraud events is low compared to overall transaction volumes), which means that missing positive fraud cases can have a significant negative impact on model quality. It also means that some potential fraud and/or fraud patterns may be missed.

A major bank is now using Hadoop to allow it to run analysis across the whole daily transaction in volume, rather than just above-the-line transactions. This has had the advantage of enhancing detection efficiency, but has also reduced the computing costs and time to run analyses.

Another key challenge in tackling fraud is that it is increasingly being perpetrated by professional fraudsters who have an understanding of fraud detection methods, and will try to game the system accordingly. This means that banks need to detect and adjust behavioral models to events with a low

degree of latency. While still at trial stage, a number of banks are looking at using Spark to support streaming of transactions with more sophisticated models in a real-time setting, with ability for models in the background be continuously updated through machine learning.

Looking ahead: Big Data becomes key to managing misconduct risks and detecting new forms of financial crime

Our research shows that a majority of banking institutions are now using or actively considering using Hadoop as part of their compliance management and anti-financial crime initiatives. As shown in figure three, 70% of banks are already using/ looking at this, Ovum expects that use of Big Data will extend significantly over the next 2-3 years.

This will eventually be realized across a number of use cases. Key emerging uses include:

- Its ability to support banks in tackling conduct risks by detecting trends across multiple data types;
- The ability to reduce false positives levels for AML and fraud through use of additional data sets, and more complex real-time analysis; and
- Use of unstructured data and faster analysis to improve know-your-customer (KYC) capabilities for enhanced customer-due-diligence.

Ability to work across multiple data types to become key for tackling insider misconduct risks

An important challenge for banks in ensuring compliance is that to various degrees employees will be aware of an institution's controls and compliance processes. Given this knowledge, this means there is a danger that employees may be able to circumvent controlling systems to allow them to undertake undesirable activity, such as deliberate insider fraud or wider potential misconduct (which may be or may not be deliberately malicious). Banks can try to impose more stringent controls, but there always needs to be a balancing act between rigor of controls and ensuring that employee can actually conduct their core business activities as well.

To address this, banks need to conduct analysis at multiple levels, to identify compliance or risk flags that might not be triggered at an individual transaction level. For example, analysis of sales activities might find that a financial advisor might sell a disproportionate amount of business in one product set compared to an institution's average, which might suggest potential mis-selling activity even if individual compliance file-checks for the sold activity are passed. The challenge here is that an outlier in itself is no evidence that misconduct has actually occurred, and as misconduct is a relatively rare event, identifying and calibrating appropriate key risk indicators (KRIs) is problematic. This is particularly as any ensuing investigation may cause changes the flagged behavior, for example, the advisor may adjust their sales balance, without necessarily addressing the fundamental misconduct issue.

In this situation, being able work across multiple data types, rather than rely on pre-identified KRIs can be highly effective for tackling misconduct risk. In particular, this includes being able to move beyond transaction data (of which insiders may have more knowledge) to include machine generated and unstructured data. This may include system access logs, phone call data, email, or chat data. These are often investigated post-event, to substantiate details of known misconduct, but use of Hadoop-based system provides the ability to store, link, and analyze across the data sets (along with KRIs) to provides a far more effective analysis to identify potential misconduct upfront.

Reducing AML/fraud false positives through correlating activity across data sources

Similarly, the ability to combine multiple data sources and types offers significant advantages for reducing false positive levels in identifying suspect AML/fraud cases. Figure two in the first section of the paper highlighted the value of this, being a key driver of IT investment already to minimize the customer inconvenience it can cause. More effective detection also has major benefits from an operational cost perspective as reduces investigation time spent on genuine/legitimate activity.

It is also beneficial for regulators and anti-crime authorities; for example, it enhances the quality of Suspicious Activity Reports (SAR) that institutions have to submit when dealing with suspect cases. This has been a major pain-point for many countries with SAR volumes increasing significantly as regulators have reinforced requirements, particularly when a more rule-based approach has been adopted. Institutions have generally taking highly risk-adverse approach to avoid potential compliance breaches, resulting in a high number of SARs for what is actually legitimate activity, with high volumes reducing their effective value to law enforcement agencies.

Use of new data sets, such as social network data or location data allows institutions to obtain additional correlating data to facilitate automated validation/analysis of identified suspect activity through transaction-based detection models. Such data can either be fed as extra inputs into initial monitoring processes, or used as a second detection layer where activity receiving certain risk scores can be re-screened using enriched datasets. Examples here include use social link analysis to understand any associations that may affect risk assessment, or location data from social networks/digital banking sessions to help assess whether a transaction is genuine. With this approach institutions can validate activity that would fall below the bar set for internal investigation, providing greater protection against potential undetected activity.

External unstructured data becomes key for enhanced customer-due-diligence

Another key area where the Hadoop ecosystem will be beneficial is in meeting Know-Your-Customer requirements (KYC), particularly for clients where banks have identified the need for enhanced customer-due-diligence (CDD). This is typically required for clients identified as higher-risk based on factors such as size of funds, potentially suspect activity, location, or being a politically exposed person (PEP). Here banks having a greater duty of care to verify identify, establish source of funds, monitor transactions/activity, and track the customer/entity to ensure that CDD information is kept up to date. This may include both the client, and their family and known close associates (such as is required for PEPs).

While commercial supporting services do exist in this space, these are generally not regarded as sufficient by regulators, and banks need to ensure that they maintain current information on such clients, as well as react to negative events. This means that banks need to track news/media reports (potentially involving text, photos and video), social media, and relevant authority information (e.g., arrest warrants, criminal charges, or bankruptcy). Currently, this requires a high degree of manual KYC activity given much of this information is unstructured, potentially with inferred rather than direct association to the client.

With the ability to work with unstructured data, using Hadoop as a platform will significantly improve both the efficiency and effectiveness of enhanced CDD operations. Institutions will be able to automate a far higher proportion of the required monitoring and analysis, allowing them to incorporate additional external information sources and react faster to events. It also supports tools that allow patterns to be found and tracked across data types and relationships, such as social link analysis,

which means that institutions can be more effective in identifying and understanding implications of associates.

Appendix

Methodology

ICT Enterprise Insights presents the data from more than 6,275 interviews of CIOs and other senior IT decision-makers conducted between August and October 2015. The survey covered more than 60 countries worldwide, looking at industry technology trends across the financial services, telecom and media, public services, and energy sectors.

The data was subject to industry-leading levels of rigor. Respondents were drawn from panels of pre-qualified CIOs/senior IT decision-makers who then had to clear a series of screener questions set by Ovum. Interviews were conducted in the respondent's native language where English was not commonly spoken and administered online or via telephone. The resulting data was reviewed by Ovum's primary research analysts as well as our sector experts, using quality assurance tools developed by Ovum.

Author

Daniel Mayo, Chief Analyst, Financial Services Technology

Copyright notice and disclaimer

CONTACT US

www.ovum.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo