MarkLogic®

Financial Markets Essentials: Staying on Top of the Market

MARKLOGIC WHITE PAPER

This white paper draws on extensive research and forward-looking statements affecting financial markets. We have consolidated five major trends and provide a comprehensive overview of how our capabilities are best placed to help our clients stay on top of them and shape the financial markets architecture in the next decade.

Contents

EXECUTIVE SUMMARY

It has become a tradition for leading management consultants to publish the industry look-ahead. We have taken our own stab at consolidating and analyzing key trends in financial services and coming back to the markets we serve with a concise overview of MarkLogic's capabilities best placed to help stay ahead of these trends not just for this current year, but with a longer-term perspective. Our ambition is to help our clients shape financial markets architecture for the next decade.

Below are the top five trends we believe will be shaping financial markets:

- FinTech disruption and battling for customers
- Digitalization and enhanced customer experience
- Integrated GRC
- Moving to the Cloud
- A shift in the markets paradigm: Cyber and Data security

Like our clients, MarkLogic continues to invest in our core technology, and today we are best positioned to help our customers stay on top of the market.

FINTECH DISRUPTION AND BATTLING FOR CUSTOMERS

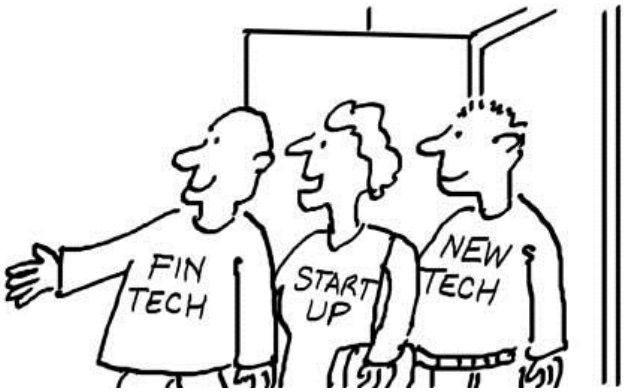
According to a recent Capgemini survey, "fintech players are causing disruption and disintermediation, often targeting discrete highly profitable segments of the banking value chain."[1] Similarly, FinTech was noted as a high priority concern by 71% of participants in a PwC survey of 500+ executives from financial institutions in 17 markets.[2]

Indeed, FinTech startups are targeting specific services where they can build up market share with lean, agile platforms, establish an online and mobile presence rapidly and erode the margins of major institutions. Unencumbered by legacy systems and high fixed costs, these challengers can engage customers and build loyalty with a select but innovative product set. For instance, N26.com is a new modern retail bank which has just gained full accreditation from the CEB for both payment and credit. So, a group of 30 people has been able to get a full operating bank with European ambitions in less than three years of existence.

In a heavily regulated industry such as the financial markets, the appropriate response by the incumbents may be to set up subsidiary start-ups to meet the new competition in each category. The Innovation Labs set up internally by Deutsche Bank, Morgan Stanley, BNY Mellon, and Barclays may be the vehicle to meet challenger threats faster and at lower cost.

1 Capgemini, Top 10 Trends in Banking in 2016

2 https://thefinancialbrand.com/56988/retail-banking-strategy-2020/



Regulators are tracking these developments, and as they grant charters to the new challengers they also focus on meeting their supervisory obligations in the face of emerging technology and business models. It may not take long to have standards for access APIs specified by regulators to support on-demand audits, financial forensics, and operational surveillance. Such an API could be executable in a secure and privileged environment as the optics for oversight purposes. As technology enables new business and regulatory models in a more operationally sound and reliable manner, the adoption rate is expected to accelerate in major institutions.

Incumbents still have advantages because of decades of experience supporting customer needs and deep knowledge and experience with regulatory and business issues. However, they are held back by systems developed for an earlier age in which the focus was on optimizing systems from a business unit or application perspective instead of focusing on firm-wide capabilities. The most significant issue is that data generated and used by individual applications is maintained in proprietary silos instead of being easily accessible firm-wide.

Competing with new platforms requires the need to construct a holistic view of all data to support the product line with 360-view data and provenance, backed by enterprise scale features such as security, scalability, and resilience. The FinTech challenge cannot be adequately countered by incremental enhancements or transformations of the existing data center infrastructure. At the same time, large financial institutions need to ensure business continuity while investing into and implementing innovative technology.

A SHIFT IN THE MARKETS PARADIGM: CYBER SECURITY IS ALL ABOUT DATA

Insider threat is a pervasive security problem for financial markets, and has been since organized trading began. While various technology solutions have been used to deal with threats from outside the enterprise perimeter, inside threats have not always been guarded against and the best-practices to remediate them are a moving target. In fact, when organizations work with contractors and subcontractors, arms-length corporate entities, and necessarily have to share information with their supply chain and trading partners, a concrete concept of what is “Inside” and what is “Outside” is increasingly elusive.

International Data Corporation forecasts the cyber security market hitting $100,000,000 (US) per year. Most investment in this area has been on perimeter, network, application, and endpoint security. The industry has also created specialized threat intelligence and monitoring solutions. Meanwhile, innovation and investment around data security, particularly at the database level, has not kept up. The result is that organizations across government and industry have created a hard shell and a soft, potentially vulnerable middle.

At the same time, a large and complex organization, comprising multiple communities of interest, using siloed information systems, procured and implemented over years or decades, may have several related risk, threat, and security initiatives. Furthermore, these Risk Management, Insider Threat, Supply Chain Safety, Threat Management, Facilities security, and other initiatives themselves are creating data silos.

To monitor potential instances of insider threat there needs to be a method of indexing not only all of the data but all of the interactions. With this, security teams can establish patterns of normalcy and anomalous behaviors in terms of data access, query and download, communications (forwards and cc'ing), and the temporal – and even geospatial – aspects of these patterns.

The US National Institute of Standards & Technology circular 800-53 on access controls declares, "A state of access control is said to be safe if no permission can be leaked to an unauthorized or uninvited principal."[3] This safety is achieved through separation of duties, Role- or even Attribute- or Policy-based Access Controls based on need-to-know, competence, authority, obligation, or conflict-of-interest factors. Additionally, data redaction and masking capabilities need to be in place to allow functions like reporting, development, and quality testing to occur efficiently without exposing personal data.

RELATIONAL CAN NO LONGER ANSWER YOUR BUSINESS NEEDS

Relational database management systems (RDBMS) have supported the explosion of IT solutions – including security solutions – over the past several decades. However, they cannot keep up with the volume and variety of data that's now being produced. Schema maintenance is difficult and time-consuming leading to development delays. Not only is it a struggle with the structured data that is traditionally used in relational databases, but incorporating the huge volumes of unstructured data that's now available requires enormous effort on the part of IT departments to extract, transform, and load before the data can be used. Then, add on the work needed to manage and integrate data sources, predefine queries, and build the analytical applications used for big data, and you have more data silos with more data risk.

BIG DATA TOOLS ONLY ADDRESS PART OF THE PROBLEM

A big data approach may go part of the way to solving the problem for the insider threat. It can help with the task of separating the large volume of irrelevant data from the more valuable information – but it still requires data analysts to examine that and apply context. Many big data approaches are also weak in security.

This weakness often extends to the point where they cannot identify what data needs to be protected, making it almost impossible to build a secure system.

It's the same kind of situational awareness problem that the US Department of Defense (DoD) has struggled with for years. The DoD uses big data techniques to collect inputs from multiple sensors and systems in order to analyze activities and develop intelligence it can use for its operations. However, analysts still spend most of their time assembling known data. A similar problem exists in financial markets, especially in the context of multi-jurisdictional Governance, Risk and Compliance programs. What we are seeing now is that most of the financial markets players take a retrospective view of complying with a specific regulation.

WHEN IS ENOUGH TOOLING ENOUGH?

We believe that it's now that financial markets should adopt a new approach to solving their insider threats, based on situational awareness. This means a shift of focus to data security. Making sure that your organization has a 360 view of secure data is essential. You can search it, analyze it, interpret it, and make it available both for reporting needs, customer insight, and operational excellence.

3 http://www.nist.org/nist_plugins/content/content.php?content.18

Market research shows that more than 50 percent of security breaches are the result of a careless employee. This presents companies with three major risks:

- Compliance fees as regulations continue to tighten up with regards to data privacy; GDPR coming into effect in May 2018 is just one example
- Brand and reputational damage, especially if a lawsuit takes a company to court and into the media headlines
- While the financial industry, especially in the mature markets, is fighting for customer retention, customer churn is increasing as consumers are empowered to know and make data privacy requests at any time

Of course, to minimize the impact of data privacy breach due to human error requires adequate legal and compliance policy and education of employees. New technology can help mitigate those risks thanks to role-based and compartment-level security settings. This is important to ensure that data is only shared with individuals or organizations that have consent from the citizen to whom the data pertains. For example, if I – as a customer – withdraw consent for direct marketing, it is important to restrict my personal data from marketing department processes that generate campaigns. Legally, it may also be a requirement to delete personal data from word documents and spreadsheets as well. Encryption at rest is another important element that ensures that even if a data breach occurs, the data is secure.

DIGITALIZATION AND ENHANCED CUSTOMER EXPERIENCE

According to McKinsey, "digitization is impacting banks in three major ways. First, regulators, who were initially more conservative about the entry of nonbanks into financial services, are now gradually opening up. Over time, huge tech companies may be able to insert themselves between banks and their customers, capturing the vital customer relationship and presenting an existential threat. On the positive front, a number of banks are teaming up with FinTech and digital firms, using big data and analytics to sharpen risk assessment and drive revenue growth. Lastly, many banks have been able to digitize processes and dramatically lower costs in their middle and back offices (although digitization can sometimes add costs)."[4]

Indeed, embracing the digital channels to engage with customers today is no longer a nice-to-have. And we believe this challenge is solved if banks address it at the data level rather than the application level. Being able to aggregate data across multiple systems into an operational data hub provides great business advantages to multiple functions across the financial institution, delivering data for best-in-class analytics as well as supporting any number of operational use cases. Embracing a data-centric integration perspective – vs. point-to-point application integration – makes your organization flexible enough to respond to new opportunities at the speed of business.

4 McKinsey, A Brave New World for Global Banking: McKinsey Global Banking Annual Review 2016

CUSTOMER CENTRICITY

The rise of social media has created many opportunities for companies to engage better, faster and more frequently with their customers and gain richer insights. But it hasn't – in many instances – enabled them to fully embrace customer centricity. As reported by MarketingProfs,[5] research by the CMO Council in collaboration with SAS has shown that 40 percent of the marketers and 51 percent of the IT employees surveyed viewed Big Data as critical to the ability to develop and execute customer-centric programs. However, 52 percent of the marketers and 45 percent of IT professionals said that data that is in silos across an organization makes it difficult to truly achieve customer-centricity. What's important to recognize about this data is that it comes in many shapes and sizes; whether relational data coming from a CRM system, legal documents, web data, or marketing pdfs.

Having a system that can process any shape of data is important in bringing silos together and creating a truly 360-degree view of that data. Traditional relational systems will struggle with this variety of data.

Financial markets are highly interconnected. Global operations, dispersed teams, multi-jurisdictional rules and business practices make it critical to embrace a geospatial view of the data which exists across the organization. Geospatial tracking has been leveraged by the government agencies and can be applied to financial institutions.

Legacy geospatial databases are unfit to manage unstructured information: documents, observations, human geography, or situational awareness. Too often a geospatial database plus a spreadsheet becomes the de facto system of maintaining real-time data, leaving analysts to manage and search geospatial features and institutional knowledge in separate locations. With most geospatial teams managing hundreds to thousands of data sources, the problem is compounded by having to search a geospatial system and numerous feature-related flat files. It is impossible to exploit all of an organization's geospatial data in a unified perspective with current geospatial systems.

Situational awareness in financial markets is becoming a critical success factor. Technology must not only answer questions you already know, but be able to answer those you don't. And these questions may come from various parts of the world. The type of questions asked of data change too; consider that 15% of the queries Google sees on a daily basis have never been searched before, according to CNet.[6]

INTEGRATED GRC

Following the financial crisis of 2007-2009, financial markets have become the most tightly regulated industry in the world. Regulations vary across jurisdictions, and global players have set aside huge budgets to enable their GRC functions. However, according to Capgemini, a significant portion of bank's risk management is still fragmented and manual – which makes it difficult to comply with ever changing regulations.[7] And we need to consider the cost implications too. According to Thomson Reuters, compliance spend in the past two years has increased by 60% in North America, 75% in Europe and 80% in the Middle East.[8]

With a growing customer base, an increasingly global emphasis, and a harsh compliance environment, financial services firms need GRC solutions that provide a better understanding of risk and a complete view of the customer.

A successful governance, risk, and compliance (GRC) strategy for financial services firms requires a comprehensive approach to data management. Today, they must be able to integrate structured and unstructured data from internal and external sources. Looking at data as a whole allows financial services firms to:

- improve strategic business decisions in response to market risks and opportunities
- use proactive and effective monitoring of the changing regulatory landscape
- increase the efficiency of their organizations and lower the cost of compliance
- avoid fines, penalties, and damage to reputation
- maintain a 360-view on risk and customer data within their organizations

5 http://www.marketingprofs.com/charts/2013/10574/marketing-and-it-big-data-an-obstacle-an-opportunity-and-key-to-customer-centricity

6 https://www.cnet.com/news/google-search-scratches-its-brain-500-million-times-a-day/

7 Capgemini, Top 10 Trends in Banking in 2016

8 Thomson Reuters, What's Compliance Worth, 2016

LEGACY DATA SYSTEMS STRUGGLE TO MEET GRC NEEDS

Data stored in legacy systems spread across departments and locations complicates GRC processes. This data includes new customer background data, customer contractual agreements, communication logs, and more. In addition, content from social media, instant messaging, forum usage and unstructured data from other sources increases the information that grows outside of transactional systems.

Pulling data from architecture that relies on a traditional relational database approach is complicated, costly and time-consuming, and as soon as a source changes or a new source has to be integrated, the process and models need to be redefined.

This makes it difficult for analysts and internal GRC teams to have timely access to information on the risk profile of new customers, conduct business planning, and meet GRC mandates.

PROCESSING FINANCIAL SERVICES DATA REQUIRES TECH CHANGES

In the aftermath of a succession of crises, the financial services industry has undergone a decade-long consolidation and is doing so under ever more constraining regulatory regimes.

Hence, the response to the waves of regulatory requirements will need to include tackling the data management infrastructure, and that process will have to start with moving data out of silos and incorporating the content that is generated by other sources such as social media.

A solution architecture that incorporates all types of data stored across systems enables financial institutions to obtain a 360-view of their data relating to risk, customers, and trades. It also facilitates e-discovery. Beyond compliance, integrated data is critical for monitoring and making informed decisions, especially when coupled with BI tools.

Conventional ETL-heavy processes inevitably cause delays as data needs to be identified, aligned, and transformed. Solving the data challenges – and subsequent development lifecycles – just cannot be achieved with these technologies.

Organizations deploying an operational data hub architecture find that the time to market and implementation schedules are significantly lower than when using traditional approaches, providing operational efficiency at an enterprise level.

MOVING TO THE CLOUD AND HOW TO STORE YOUR DATA

More and more organizations are turning to the Cloud for more cost-effective IT infrastructure. Cloud infrastructure – like that provided by Amazon Web Services (AWS) and Microsoft Azure – is proven to be scalable, reliable, and secure, and can help improve data accessibility (including better support for a mobile workforce).

The migration to and operations on Cloud platforms will be more efficient and cost effective if data consolidation, integration, and aggregation have already been achieved with discovery and analytics capabilities on a multi-model platform. Migrating a highly distributed and fragmented set of systems creates additional operational and investment risks.

The cost of running apps in the cloud is currently low. But, will that always be the case? Most databases are purpose-built for one environment and firms must choose up front which environment to deploy in. If they want to make a

change later, they may have to buy additional licenses. Worse, they may need to re-write their application. The right solution is to use database technology that can run anywhere: on-premises, virtualized or in any cloud environment; this ensures your organization avoids lock-in.

DATA STORAGE

In today's new regulatory environment firms are required to track far more information than in the past and to maintain it longer. Some information needs to be accessed regularly. Other data may never be accessed and is stored on a contingency basis. As data ages, it often needs to be accessed less and less.

Treating all this data as having the same data access requirements will result in overspending with minimal efficiency gains. From the cost efficiency perspective, utilizing a tiered storage strategy is an effective way to remove less used data from high SLA platforms and significantly reduce operational costs. Tiered storage provides the ability to store and manage data in different tiers based on cost and performance trade-offs—whether it's flash storage, traditional local or shared disk storage, HDFS, or cloud storage.

RELATED MATERIALS

Explore online to find answers on how the MarkLogic technology can help your organization.

www.marklogic.com/solutions/financial-services

MARKLOGIC CORPORATION
999 Skyway Road, Suite 200 San Carlos, CA 94070
+1 650 655 2300 | +1 877 992 8885 | www.marklogic.com | sales@marklogic.com

999 Skyway Road, Suite 200 San Carlos, CA 94070
+1 650 655 2300 | +1 877 992 8885
www.marklogic.com | sales@marklogic.com