ISCTE Business School
Instituto Universitário de Lisboa

Bits and Bytes of Financial Regulation

Diogo Azevedo Algarvio

Dissertation submitted as partial requirement for the conferral of
Master in International Business Management

Orientador(a):
Prof. Doutor António Manuel Corte Real de Freitas Miguel, ISCTE Business School,
Departament of Finance

October 2018

BITS AND BYTES OF FINANCIAL REGULATION

ISCTE Business School
Instituto Universitário de Lisboa

Diogo Azevedo Algarvio

Acknowledgments

For years I delayed this moment, time was “never enough”.

Paradoxically in the busiest year of my life this moment finally came. Time was nothing but an excuse that validated my fear of failing. Sometimes we need to remind ourselves, or if we are really, really lucky, be reminded that giving up is the only sure way to fail.

I thankfully am very, very lucky.

First and foremost, I would like to thank my mother, a true example of hard-work, discipline and most importantly love.

To my beautiful girlfriend, when I’m feeling like Clark Kent your smile makes me feel like Superman. I hereby declare that I will keep the fridge door closed and a smile on your face. Thank you, my love.

To my grandmother, for teaching me the power of prayer and family. Thank you.

To my friends I’ll do my best to repay the beers that I’ve missed.

To Professor António Freitas Miguel, until the last second you never gave up on me. “Education is not the filling of a pail, but the lighting of a fire.” W.B. Yeats. Thank you.

To my manager Christophe and to his beautiful family, thank for your help, guidance, ideas and inspiration while I was working in New York.

I would also like to thank my employer for trusting me with the opportunity to embrace so many international projects of great interest, thus inspiring me for my dissertation.

Grandpa, wherever you are, this goes to you.

Abstract

Since 2008, banks have spent more than €342 billion on settlements, enforcement actions, and fines, and until 2020 according to Reuters this value is expected to rise to €400 billion. As a result, technological solutions were implemented to help Financial Institutions deal with the increasing compliance burden and regulators addressing the constant difficulties of enforcing and monitoring regulatory requirements to limit risks and promote financial stability. This led to the emergence of a whole new movement in the Financial Industry - Regulatory Technology.

In this dissertation, the aim is to analyze how technology can help Financial Institutions deal with risky behavior and regulatory demands in the most efficient and cost-effective way and to show how extremely complex this process can be, by following the deployment of an electronic communications surveillance tool within a top-tier firm.

Electronic communications are crucial parts of investigations such as the subprime mortgage crisis, the London Interbank Offered Rate and the currency market manipulation scandals or the COMEX gold and silver futures markets spoofing scandal. To appropriately address the nature of these threats, holistic risk assessment tools that gather these records (e-mail, chat, voice, trade logs, etc.), discover correlations and provide a credible output that necessitates supervisory review are of extreme importance.

The challenge for Front-Office Supervisors is finding the proverbial "needle in a haystack" – the combination of Email, Chats, transactions records, voice logs, and other reports – that should be flagged for suspicious activity and reviewed in conjunction with Compliance and Anti-Fraud teams.

JEL Classification: G21; G28

Keywords: Regtech; Regulation; Technology; Surveillance.

Resumo

Desde 2008, os bancos já gastaram mais de €342 biliões em acordos, ações de fiscalização e multas, e até 2020 segundo a Reuters, este valor deverá subir para €400 biliões. Como resultado, foram implementadas soluções tecnológicas para ajudar as Instituições Financeiras na superação do aumento exponencial de requisitos regulatórios, e para fortalecer a capacidade de resposta dos reguladores face às constantes dificuldades de impor e monitorizar esses mesmos requisitos com o objetivo de limitar os riscos incorridos e por sua vez promover a estabilidade financeira. O que levou ao aparecimento de um novo movimento na Indústria Financeira – Regulatory Technology (Regtech).

Nesta dissertação, o objetivo é analisar como a tecnologia pode ajudar as Instituições Financeiras a lidar com comportamentos indevidos e requisitos regulatórios da forma mais eficiente e rentável e mostrar quão extremamente complexo este processo pode ser, ao seguir de perto a implementação de uma ferramenta de vigilância de comunicações eletrónicas dentro de uma grande Instituição Financeira.

As comunicações eletrónicas são partes cruciais de investigações de escândalos financeiros, como observado na crise do suprime, na manipulação da London Interbank Offered Rate, do mercado monetário e dos mercados de futuros do ouro e prata na COMEX.

Para lidar adequadamente com a natureza destas ameaças, ferramentas holísticas de supervisão reúnem registos (e-mail, conversas, voz, registos de transações etc.), descobrem correlações e fornecem um importante e credível resultado que por sua vez requer revisão por parte dos supervisores.

O desafio para os supervisores do Front-Office é encontrar a proverbial "agulha no palheiro" - a combinação de e-mails, conversas, transações, registos de voz e outros relatórios - que deve ser sinalizada como atividade suspeita e analisada em conjunto com as equipas de Compliance e Anti-fraude.

JEL Classification: G21; G28

Keywords: Regtech; Regulação; Tecnologia; Vigilância

Index of Contents

Index of Figures

Main Abbreviations Used

4MLD – Fourth Money-Laundering Directive

AI – Artificial Intelligence

AML – Anti-Money Laundering

API – Application Interface Program

BIS – Bank of International Settlements

CBOE – Chicago Board Option Exchange

COMEX – Commodities Exchange

DLT – Distributed Ledger Technology

EMIR – European Market Infrastructure Regulation

FDIC – Federal Deposit Insurance Corporation

FSB – Financial Stability Board

FX – Foreign Exchange

G20 – Group of 20

GDPR – General Data Protection Regulation

ICE – Intercontinental Exchange

IT – Information Technology

LIBOR – London Interbank Offered Rate

LOD – Line of Defense

MIFID – Markets in Financial Instruments Directive

ML – Machine Learning

NLP – Natural Language Processing

NSA - National Security Agency

P&L – Profit and Loss

PSD – Payments Service Directive

RPA – Robot Process Automation

SAAS – Software as A Service

SWIFT – Society for Worldwide Interbank Financial Telecommunication

VAR – Value-At-Risk

VIX – Volatility Index

1 Introduction

Crisis trigger adaptation processes, we readapt ourselves with new attitudes and behaviors. The 2008 Global Financial Crisis produced new problems and challenges, forcing upon us a shift of paradigm to avoid a similar downfall in a near future.

Until 2008, the financial sector was enjoying a decade of benign economic conditions, only disrupted by a decline in economic activity in the early 2000s. Banking conditions seemed very reassuring with six consecutive earning records for the industry's top players from 2001 to 2008 (Klein, 2017).

Public and the Private sectors greatly underestimated the risks that we were facing. The economic boom that occurred in the first 2000's massed to a significant build-up of risks. The banking agencies did not recognize the full extent of these risks, and the regulatory framework did not provide adequate safeguards for financial stability. Markets and regulators had to discover that they failed to recognize one risk, "systemic risk" (Klein Aaron, 2017).

The activities of Financial Institutions operating under pre-crisis rules fueled the housing bubble and contributed to the collapse of the financial system. Disproportionate use of financial leverage, inadequate liquidity, securitization of large volumes of poorly underwritten mortgages and the growth of an opaque network of credit derivatives backing those securitizations (Klein Aaron, 2017). The confluence of these factors led to the need for taxpayer's bailouts on an unprecedented scale (Klein, 2017).

Countries paid a high price for not recognizing the magnitude of risks faced in the pre-crisis years through the weakness in the banks' regulatory frameworks (Klein, 2017).

But even after the Global Financial Crisis, risky behavior persisted, and the eternal cat and mouse game carried on with the London Interbank Offered Rate and the currency market manipulation scandals or the Commodities Exchange gold and silver future markets spoofing scandal.

Since 2008, banks have spent more than €342 billion on settlements, enforcement actions, and fines, and until 2020 this value is expected to rise to €400 billion (Reuters, 2017). To further put things in perspective, on the whole, the industry spends between €900 million to €1.3 billion a year on compliance-related costs and the number of regulatory worldwide changes a bank has to deal with every day has increased from 10 in 2004 to 185 today (Reuters, 2017). That amounts to

a regulatory change that has to be interpreted and implemented every 12 minutes (Reuters, 2017). But not only the cost side is at stake, Quinlan and Associates a Hong Kong-based financial services consultancy firm also estimated that risky behavior had erased $850 billion in profits for the top 50 global banks since 2008 (Reuters, 2017).

Increasing compliance costs and regulatory requirements made the use of innovative technologies a natural and promising solution not only for Financial Institutions but also regulators. (Arner, Barberis, and Buckley, 2017 a).

One example is the race between evolving compliance demands and conduct risk, which exposes organizations to severe reputational losses and fines. Powered by artificial intelligence, machine learning, deep learning, and advanced analytics, institutions can now structure unstructured data (attachments files, the content of web searches, emails, corporate chats, etc.) to fully comprehend the true context of all types of communications and prevent insider threats of doing considerable damage.

In this dissertation, the aim is to analyze how technology can help Financial Institutions deal with risky behavior and regulatory demands in the most efficient and cost-effective way and to show how extremely long and complex this process can be, by following the deployment of an electronic communications surveillance tool within a top-tier firm.

The remainder of this dissertation is structured as follows. Section 2 presents the literature review. It starts by examining how regulatory advances can help in the prevention of regulatory issues covering the history of financial innovation until the 2008 Global Financial Crisis. This section then proceeds with the impact of the Global Financial Crisis and the Post-Crisis reforms that followed, describing new technological advances that surfaced to help institutions and regulators deal with the increasing compliance burden and the overall risky behavior that led to astronomical fines and consequent reputational damage.

In Section 3 we evaluate the downside of poor electronic surveillance mechanisms within the financial sector and the need for a multi-vector surveillance tool in the industry, setting the foundations for the in-company project. After several regulatory fines, *Player1*, as it's going to be called for confidentiality purposes, decided to replace its electronic communication surveillance tool to meet United States regulatory demands.

Section 4 presents a map for the in-company project and the respective research questions, outlying the specific issues of *Player1* and steps to take in the search and deployment of a holistic

surveillance tool. The analysis of the information will be conducted throughout Section 5, from defining the business requirements to meeting with other *Players* and vendors in the market, to the decision and conduction of a Proof of Concept. This section is complex in its nature, despite best efforts to simplify the technical aspects of the in-company project they are crucial in order to understand the difficulties and limitations of such a considerable project.

Section 6 will describe the implementation of the solution and Section 7 will present overall conclusions for the in-company project. Finally, Section 8 will conclude the dissertation.

2 Literature Review

Technological advances are changing the financial landscape at an unforeseen rate. But with new opportunities, new risks also arise. New regulatory approaches must be developed by Financial Institutions and regulators, thus keeping a valuable balance between innovation and financial stability.

In November 2015, the Financial Conduct Authority (conduct regulator for the United Kingdom) issued a Call for Input requesting views on how it should handle Regulatory Technology describing Regtech as a "sub-set of Fintech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities." (Arner, Barberis and Buckley, 2017a: 381).

Arner, Barberis, and Buckley (2017a) argue that this view is overly narrow, in the long run, while Fintech is inherently financial in its focus, Regtech has the potential for application in a wide range of contexts (Arner, Barberis and Buckley, 2017a). Even though this dissertation has a financial focus, in the future Regtech may be applied to all sorts of different areas, like environmental compliance monitoring or tracking the global location of airliners on a real-time basis (Arner, Barberis and Buckley, 2017a).

The literature review starts by covering the history of financial innovation until the 2008 Global Financial Crisis, an event that changed the financial world as we know it according to authors such as Arner, Barberis, Buckley and Zetsche (2017). This section then proceeds by studying the impact of the Global Financial Crisis and the Post-Crisis reforms that followed as a prologue for the surge of Regtech. Ending with describing new technological advances that surfaced to help institutions and regulators deal with the increasing compliance burden and the opportunities and challenges that this new industry faces.

2.1 Innovation and Financial Regulation

The launch of the calculator and the ATM in 1967 marks a period of digitization in Finance. SWIFT, the Society for the Worldwide Interbank Financial Telecommunication, which provides protocols to enable communications between domestic digital payment systems, was established in 1973, followed soon after by the collapse of Herstatt Bank in 1974, a privately held German bank that went bankrupt due to wrong bets in the direction of U.S. dollar in a famous incident that

illustrated the risks of international finance (Arner, Barberis and Buckley, 2015). German regulators forced closure on the bank on 16:30 in Germany which in turn was 10:30 in New York, as a result the bank ceased operations between payment times and the counterparties did not receive their respective U.S. dollars payments, coining an alternative term to settlement risk known as Herstatt risk[1] (Arner, Barberis and Buckley, 2015).

This event proved that with markets becoming increasingly global, local regulations were ineffective to address the trials of international finance. As a result, the collapse of Herstatt Bank served as the catalyst for the first major regulatory initiative: the establishment in 1975 of the Basel Committee on Banking Supervision of the Bank for International Settlements (BIS) (Arner, Barberis and Buckley, 2017b).

The historical background of financial regulation is in its essence a story of regulatory initiatives in response to a crisis. An example, is the financial liberalization and deregulation of the 1970s followed by the Latin America debt crisis in the early 1980s (Arner, Barberis and Buckley, 2017 a). The Latin America debt crisis and the growing concerns on deteriorating capital ratios of main international banks became the driver for the first Basel Accord on capital adequacy in the late 1980s (Arner, Barberis and Buckley, 2017a). This liberalization process, followed by crisis, and then a reactive regulatory response demonstrates the unfortunate cyclical nature of regulatory reform given that prevention should be its core focus.

"The year 1987 marked a new period of regulatory attention to the risks of international finance and its intersection with technology" (Arner, Barberis and Buckley, 2015: 10). A major market crash occurred. "The "Black Monday" stock market crash showed that markets around the world were interlinked through technology in a way not seen since the 1929 crash" (Arner, Barberis and Buckley, 2015: 10). Stock markets fell deeply in Hong Kong, Australia, Spain, United Kingdom, New Zealand and the United States becoming the largest one-day percentage decline in the Dow Jones Industrial Average[2], an index that aggregates 30 large publicly traded companies

[1] Alternative term to settlement risk with particular reference to foreign-exchange transactions.

[2] Saturday, December 12, 1914, is sometimes erroneously cited as the largest one-day percentage decline of the DJIA. In reality, the ostensible decline of 24.39% was created retroactively by a redefinition of the DJIA in 1916.

in the United States. Although until today there is still no agreement on the causes of the crash, the theory is that the crash was caused by "program trading"[3] (Arner, Barberis and Buckley, 2015).

The reaction led to the introduction of a variety of financial regulatory instruments, particularly in electronic markets, to control the speed of price changes ("trading curbs" also called as "circuit breakers") thus preventing speculative gains and dramatic losses (Arner, Barberis and Buckley, 2015). It also led securities regulators around the world to begin working on mechanisms to support cooperation, in the same way that the 1974 Herstatt crisis and the 1982 Latin America debt crisis triggered greater cooperation between bank regulators on international finance (Arner, Barberis and Buckley, 2015: 11).

Further, the underlying framework for a single market in the European Union established by the Single European Act (1986) and the financial liberalization in the United Kingdom, combined with the Maastricht Treaty (1992) and an ever-growing quantity of financial services Directives and Regulations from the late 1980s, set the structure for the complete interconnection of the European Union financial markets by the early 21st century (Arner, Barberis and Buckley, 2015).

Financial Institutions expanded in scope and scale, culminating in huge conglomerates, grouped companies that provide services in at least two different financial sectors (banking, securities, insurance), leading the path for a much more interconnected financial market (Arner, Barberis and Buckley, 2017a). This took place mainly due to mergers and acquisitions, with the merger of Travelers and Citibank to form Citigroup in 1999 becoming quintessential (Arner, Barberis and Buckley, 2017a). This specific deal is attributed by some as the start of the deregulation period that led to the 2008 Global Financial Crisis, because Citi became such a diversified financial services enterprise in 1998, it was legally incompatible with the Glass-Steagall Act of 1933, the legislation that established the Federal Deposit Insurance Corporation (FDIC) and forbade banking entities from acting as both a commercial bank and an investment bank or broker (Verschoor, 2009).

[3] "Program trading" involves pre-set computerized buy and sell orders, and so when stock prices drop to a certain level, this would trigger automatic selling by computer programs, which would then trigger more price drops, triggering more sales and eventually resulting in our first major coordinated global market crash.

TABB group's report (2017) analyses this issue as many of today's large banks are the product of multiple mergers over the last 30 or so years, reflected below on Figure 1. They are saddled with complex and redundant legacy infrastructure that may not have been fully integrated.

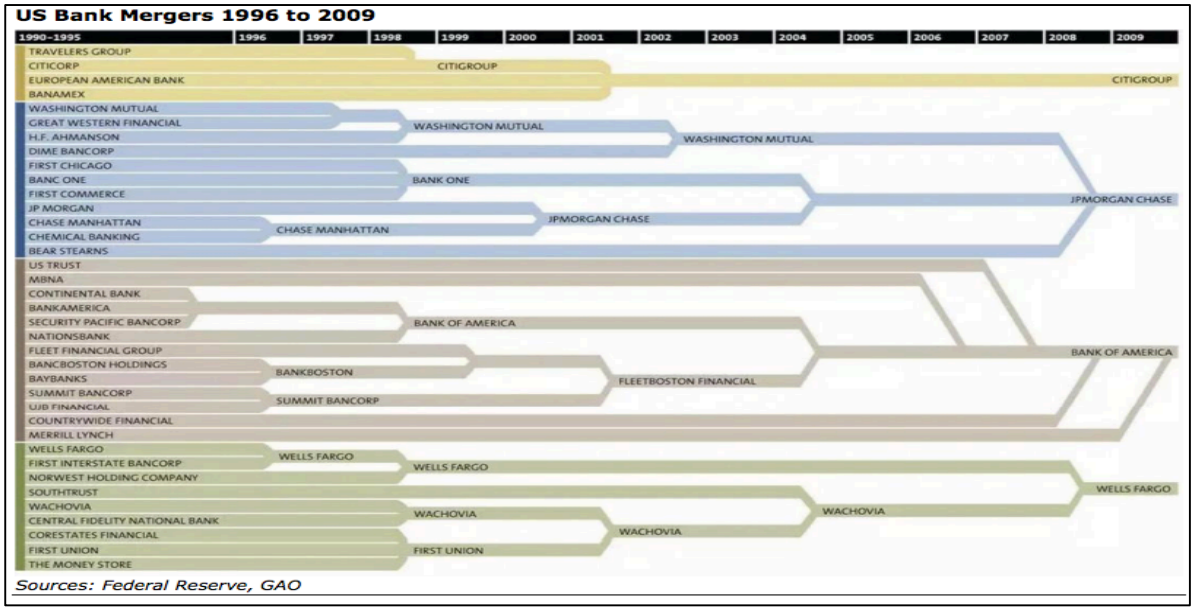

Figure 1: US Bank Mergers 1996 to 2009. Source: "TABB Group"

As institutions increased their cross-sector and jurisdictional scope, they also faced many new regulatory challenges.

According to Arner, Barberis, and Buckley (2016), the first iteration of Regulatory Technology appeared through the 1980s and 2000s risk and management teams with the combination between quantitative finance and information technology reflected itself in the Value At Risk (VAR) systems in Financial Institutions. Software systems developed by J.P Morgan, subsidiaries of Reuters and other vendors were part of a set of tools that enabled participants in the financial markets to estimate their exposure to market risk (Risk Metrics Technical Document, 1996). The issue was that the sector, including regulators became over-confident with the aptitude of this quantitative IT framework for risk-management purposes, as it was shown by the heavy reliance of the Basel II Capital accord on these risk-management systems for Financial Institutions (Arner, Barberis, and Buckley, 2016 a).

2.2 Global Financial Crisis: 2008

Prior to the 2008 Crisis, regulatory approaches to financial innovation were framed as "restricted" or "permissive". Arner, Barberis, Buckley, and Zetsche (2017) suggest that while crises might be more common in more permissive systems, over the medium to long term the benefits in terms of growth and development outweighed the costs of periodic crises.

The efficient market hypothesis states that markets will price assets with all the information available and therefore parties can make decisions on how to efficiently allocate their resources.

This hypothesis led to a general consensus for market-based approaches to financial regulation, even though it is based upon a number of perfect market assumptions, such as costless information, no transaction costs, that investors have homogeneous expectations and are rational. In theory, these ideas would therefore lead towards efficient financial markets and proper support of the overall economy (Arner, Barberis, Buckley, and Zetzsche 2017).

The issue was that even before 2008, it was known that information is not costless, there are transaction costs in acquiring information or enforcing transactions in markets, and that investors don't have homogeneous expectations.

Although regulation would be used to help markets function in a better way, the 2008 crisis and the billions of dollars spent in bailouts highlighted a much bigger problem which is called systemic risk (Lin, 2016). Comparable to the 1929s and 1930s Great Depression, the collapse of an individual Financial Institution caused the collapse of the entire financial system, which resulted in an economic collapse.

"In the wake of the 2008 Crisis, the dominant permissive paradigm has of necessity been subject to reconsideration, with the regulatory pendulum going from one extreme to the other" (Arner, Barberis, Buckley and Zetzsche 2017: 49).

Market efficiency could be increased by innovation, thus delivering new solutions to old problems, including financial exclusion and the quality of consumer decision-making to make markets global complete with improved risk-sharing. Although, as seen with derivatives and securitization, financial innovation can bring new risks, due to their characteristics they are also indispensable to risk transfer and financial management purposes (Arner, Barberis, Buckley and Zetzsche 2017).

It was in the Post-Global Financial Crisis environment that Regulatory Technology developed to the stage it's in today. Increasing compliance costs and regulatory requirements made

the use of innovative technologies a natural and promising solution not only for Financial Institutions but also regulators. (Arner, Barberis, and Buckley, 2017a).

2.3 Post-Crisis Reforms

"From 2008 up to approximately 2016, regulatory requirements at the international level, such as the United States and the European Union, were dominated by the necessity to reregulate the financial system, to prevent future financial crises or at least to put in place new regulatory frameworks which would have prevented or alleviated the 2008 Crisis" (Arner, Barberis, Buckley and Zetzsche 2017: 49).

And as crises and scandals become bigger, so do the regulatory responses to them. For example, the Glass-Steagall Act of 1933, which was implemented following the Great Depression, only ran 37 pages. Contrarily, Dodd-Frank, the United States bedrock law to prevent a future financial breakdown contained 848 pages with other thousands of additional rules (and still much more forthcoming) (Lin, 2016).

"It has been estimated that it would take businesses over twenty-four million workers' hours to comply with the demands and requirements of the Dodd-Frank rules. Also, Dodd-Frank's "Volcker Rule" relating to risky proprietary trading[4] alone is contained in 964 pages, including an 893- page preamble. This specific segment involved 18,223 comments and 1,238 days of rulemaking" (Lin, 2016: 167).

As such, the overreliance in lengthy regulations led to massive compliance costs across the industry, not only for the regulated but for the regulators, as the increasing regulatory complexity requires greater granularity, precision and frequency in data reporting, aggregation and analysis (Arner, Barberis and Buckley, 2016).

Examples are shown in the case of capital and liquidity regulations under Basel III, stress testing and risk assessments or the reporting requirements imposed on Over the Counter derivatives transactions resulting from Group of 20 (G20) and Financial Stability Board (FSB) agreed approaches in the context of United States Dodd-Frank or the European Union European Market Infrastructure Regulation (EMIR) (Arner, Barberis and Buckley, 2016).

4 The practice of banks trading for themselves rather than for clients.

According to Reuters, the number of regulatory changes a bank has to deal with every day has increased from 10 in 2004 to 185 in 2015. That amounts to a regulatory change that has to be interpreted and implemented every 12 minutes. "The European Union's Markets in Financial Instruments Directive II (MIFID II) runs into 30.000 pages and 1.5 million paragraphs, making it an immense task to understand the directive" (The Irish Advantage, 2018: 9).

According to the London-based Regtech council in the five years following 2012, more than 50.000 regulations were published across the G20. Traditional compliance tools were and are still ill-equipped to deal with this regulatory surge (The Irish Advantage, 2018: 9).

This complex and fragmented regulatory framework displayed across markets has given rise to additional compliance burdens (Arner, Barberis and Buckley, 2016). Global policymakers push for similar post-crisis reforms, but requirements and rules for implementing these can be similar or very different, overlap and contradict, which led to the financial sector turning to Regtech for optimizing compliance management (Hill, 2016).

The Global Financial Crisis damaged banks' profits and competitiveness, and the consequent regulation drove compliance costs to record highs while simultaneously restricting credit. (Arner, Barberis and Buckley, 2017b: 6). Reported by Let's Talk Payments, "the annual spending by Financial Institutions on compliance is estimated to be in excess of US $70 billion." (Arner, Barberis and Buckley, 2016: 389). Since 2008, banks have spent more than €342 billion on settlements, enforcement actions and fines, and until 2020 this value is expected to rise to €400 billion (Reuters, 2017).

But not only the cost side is affected by misbehavior, according to a study by the World Economic Forum performed in 2012, on average more than 25 percent of a company's market value is directly attributable to its reputation. Quinlan and Associates a Hong Kong-based financial services consultancy firm estimated that risky behavior had erased $850 billion in profits for the top 50 global banks since 2008 (Reuters, 2017). In a highly connected world for customers, operations, supply chains and internal and external stakeholders, reputations can be jeopardized with just a few keystrokes (Deloitte, November 2016).

But even after the Global Financial Crisis, risky behavior persisted, and the eternal cat and mouse game carried on with the London Interbank Offered Rate and the currency market manipulation scandals or the Commodities Exchange (COMEX) gold and silver futures markets

spoofing[5] scandal. The race between evolving compliance demands and conduct risk continues exposing organizations to severe reputational losses and fines.

As a result, countless reviews have been implemented to assess how Financial Institutions managed risks today. Most reviews showed weak governance and lack of a robust risk and control environment. Financial Institutions failed to demonstrate that those accountable for bringing in risks clearly understand the importance of the unmitigated exposure their institutions are currently facing. In addition, those in charge of overseeing such behaviors were equally unaware and ill-equipped (Price Waterhouse Coopers, 2018).

These findings prompted a re-examination of the 'three lines of defense' within Financial Institutions: 1st Line of Defense (Management controls and internal controls measures), 2nd Line of Defense (Compliance, Risk Management, Financial controllers and Inspection) and 3rd Line of Defense (Stakeholders with respect to risk issues and the responsibility/ accountability to provide effective oversight of the enterprise's risk profile) (Price Waterhouse Coopers, 2018: 3). This will be important to understand the supervision framework for the in-company project.

2.4 Regulatory Technology

The first time the term Regtech was coined is attributed to Professor Philip Treleaven of the University College London, one of the authors of Fintech Futures – a report produced by the United Kingdom's Government Office for Science in 2015 (Management Today, 2018).

According to Arner, Barberis and Buckley (2017b), RegTech refers to technological solutions that streamline and improve regulatory processes.

As we saw in the previous sub-section, after the Global Financial Crisis, regulatory demands increased substantially. The amount of data regulators requested supervised entities to disclose was reached all-time highs. As a result of this, and previous risky behavior, rising compliance costs and regulatory fines became a big concern in the finance sector. At the same time, developments in data science (Artificial Intelligence and Deep Learning) were allowing structuring of unstructured data and data analytics tools were enhancing the efficiency of supervisory tools. Thus, Regtech emerged (Arner, Barberis and Buckley, 2017a).

[5] The practice of placing orders in the market with the intention to cancel these orders prior to their being filled. The practice is used to ramp prices and give false impressions of market depth.

According to the Spanish international bank BBVA, financial industry Regtech focuses on:

"The automation of manual processes and the links between steps in analytical/reporting processes, the improvement of data quality, the creation of a holistic view of data, the automated analysis of data with applications that are able to learn during the process, and the generation of meaningful reports that can be sent to regulators and used internally to improve key business decision making" (Arner, Barberis and Buckley, 2017a: 389).

It stands for a holistic approach, which provides a more accepting and technological financial regulatory culture, with a flexible and forward-thinking framework and new or revised regulation centered on technology (Transatlantic, 2017:5).

Regtech was firstly known by a few firms as a "trendy expression" within the Fintech world in 2015. Nevertheless, it has existed as a separate space since 2010, which has unmistakably developed in the course of the most recent years and pulled in a great deal of attention from the financial services industry (Alvarez and Marsal, 2018).

According to Alvarez and Marsal report (2018), from 2010 to 2016, Regtech built up a strong establishment inside the Fintech world, focusing on complex new regulations, litigation and regulatory remediation areas faced by banks and overall reduction of costs of compliance. An estimated over 300 Regtech firms were launched up till 2016.

A start-up phenomenon rose with the need to develop rapidly. Regulators were also searching for new approaches that helped to implement regulations as efficiently as possible (Alvarez and Marsal, 2018).

A case-study by Watson Financial Services, IBM, 2017 where IBMOpenPages software was deployed to enhance risk and control assessment workflows for HypoVereinsbank resulted in 33% of reduction in personnel requirements due to better use of existing resources.

Regtech not only offers banks the potential for massive cost savings in meeting their compliance obligations, but it can also offer the opportunity for regulators to perform their functions more effectively in close to real-time (Arner, Barberis, Buckley and Zetzsche 2017: 52).

Regtech firms deal with information in a way that was never seen. Data collection, monitoring, analysis and reporting evolved into a completely new industry. This was fundamentally driven by advances in big data technologies. The firms that propelled in this period managed upcoming regulations like Payment Services Directive (Open Banking), Markets in Financial Instruments Directive II (MIFID II), Fourth Money Laundering Directive (4MLD) and

General Data Protection Regulation (GDPR). By far most solutions conveyed were utilizing models around Software as a Service (SaaS) also known as software on demand and open Application Programing Interfaces (APIs) which can be thought of as a simpler way for developers to interact with different kinds of software, a protocol that allows institutions to access and retrieve information from other institutions operating software, systems or libraries in an automated way (Alvarez and Marsal, 2018).

The regulatory market is flooding with data, and as a result the whole lifecycle of policymaking, enforcement and supervision is ready for disruption with the use of cutting-edge technologies. According to Arner, Barberis and Buckley (2016), while our financial system is moving from Know-Your-Customer standards to a Know-Your-Data approach, an altogether new regulatory paradigm that will manage everything from advanced digital information to data sovereignty, similarly should advance.

While Fintech and Regtech can be confused, from a market dynamic point of view, Fintech's development can be mainly attributed to a bottom-up movement led by start-ups and IT firms. Whilst Regtech has developed as top-down response to institutional demand (Arner, Barberis and Buckley, 2017a). On an early phase of Regtech, start-ups focused more on the technology to drive compliance use cases and were less acquainted with the subtleties and regulatory complexities in a holistic way, which proved a significant challenge for banks wishing to work with them (Alvarez and Marsal 2018).

Presently, Regtech firms are expected to team up with banks and regulators to exhibit their contributions far more rapidly and as these advance from specialty suggestions to more extensive and consistent recommendations, they become in far more need of help from regulators (Alvarez and Marsal, 2018).

Financial Institutions are progressively applying technology to meet the demands of regulators, reduce compliance costs and avoid regulatory fines, particularly upon large Financial Institutions in developed markets arising from new post-crisis regulations.

On the other side, regulators are confronted with the need to use technology to address the constant difficulties of enforcing and subsequently monitoring increasing regulatory requirements and are faced with developing regulatory approaches that do not hinder development and innovation while still limiting risks to consumers and financial stability (Arner, Barberis and Buckley, 2017a).

As an example of regulatory innovation, the Securities Exchange Commission Market Information Data Analytics System (MIDAS) allows to readily perform analysis of thousands of stocks for over periods of six months to a year, involving 100 billion records at a time (Milken Institute, 2018).

Working for both sides of the fence, start-ups should be persistent in dealing with bureaucracy and long-lasting sales cycles. According to Alvarez and Marsal Regtech report in 2018, they need to enhance their regulatory insights and show unambiguously how their answers can enable the Financial Institutions and regulators to perform their jobs better than before.

Regtech can therefore help: regulators creating solutions that can cater to specific requirements; industry associations for the development of standards; Financial Institutions to test new solutions for cost reduction, compliance improvement and shareholder interest protection; Fintech and Information Technology providers to offer integrated products. So indeed, Regtech has the potential to transform compliance across the financial services industry (The Irish Advantage, 2018).

Despite the experiences of the Crisis, financial and technological innovation matters deeply, and regulators need to perform a balancing act between preserving stability, protecting consumers, and promoting innovation (Arner, Barberis, Buckley and Zetzsche 2017).

The Institute of International Finance (2016:3-4) list some of the technologies with potential to help on easing the compliance burden whilst increasing efficiency and effectiveness:

- Machine learning, robotics, artificial intelligence, big data analytics and other improvements in computerized analysis and thinking create sizable possibilities when applied to compliance. Data mining algorithms based on machine learning can organize and analyze large sets of data, even if this data is unstructured and of a low quality, such as sets of emails, pdfs and spoken word. For surveillance and monitoring advances in Data Science technologies like Natural Language Processing or Sentiment Analysis could interpret the language and the opinions expressed on a piece of text to determine the writer's attitude towards a particular topic, product, etc. Other uses for Data Science technologies could be for example Automated Fraud Detection, by identifying suspicious patterns in credit card transactions or even market abuse techniques;

- Improvements in cryptography lead to a more secure, faster and more efficient and effective data sharing within Financial Institutions, most notably for more efficient risk data aggregation processes. Data sharing with other Financial Institutions, clients and supervisors could equally benefit;
- Biometric is already allowing for large efficiency and security improvements by automating client identification which is required by know-your-customer (KYC) regulations;
- Distributed Ledger Technology, well known for Bitcoin, could in the future allow for the development of more efficient trading platforms, payments systems, and information sharing mechanisms in and between Financial Institutions. When paired with biometrics, digital identity could enable timely, cost efficient and reliable customer identification (KYC) integrated with Anti-Money-Laundering (AML) related rules;
- Application programming interfaces (APIs) and other systems allowing for interoperability in accessing and retrieving information could for example, lead to pre-determined reporting of data to regulators;
- Shared utility functions and cloud-based computing could allow Financial Institutions to pool some of their compliance functions on a single platform, allowing for performance and efficiency gains.

Emerging technologies will surely play a critical role in future-proofing Regtech solution (The Irish Advantage, 2018).

Alvarez and Marsal report (2018:7) classified the following Regtech digital use cases for Financial Institutions:

- Regulatory compliance: Gathering regulatory intelligence, mapping policies, compliance governance and automated data sharing with regulatory authorities;
- Risk management. detect market risks, monitor employee conduct for suspicious behavior and protect data from numerous cyber risks;
- Financial crime: monitor financial transactions in real-time to detect fraud, market abuse, money-laundering or terrorist financing activities;

- Identity management: Know Your Customer (KYC) procedures, anti-money laundering sanctions and anti-fraud screening.

One of the main requests for Financial Institutions is Regtech solutions capable of multi-vector analysis, with interoperability, and specific supervisory guidelines for the product's architecture (Enriques, 2017) placing compliance as a competitive advantage and not purely a cost (Wyman, 2018).

Alvarez and Marsal report (2018) collected data from 401 Regtechs, 49 Traditional vendors and 352 start-ups, and concluded that only 4% play in conduct risk and 2% on Surveillance. A Verizon report on data breach investigations conducted in 2018 showed that 77% of data breaches are a result of insiders. Although cyber-crime also plays a big role, internal data breaches have been one of the biggest threats for institutions so far, like a former National Security Agency (NSA) contractor showed the world. As a result, and if no prevention measures are taken, this number is surely expected to rise.

For how many banks they've worked with, 38% of start-ups answered with 2 to 5 clients, 27% answered 10+ clients and 17% answered 1 client, being that most were in Proof of Concept deployment model. The main challenges for the start-ups are the long bureaucracy and sales process, too many silos across the banks, lack of new digital solutions by large tech vendors and difficulty understanding new regulations.

For the type of engagements, 80% were Proof of Concept while the underlying technologies were 65% data analytics and AI, 25% robot process automation (RPA) and 20% distributed ledger technology (DLT). 91% of Regtechs have only done Proofs of Concept with banks. On average, RegTechs see a shorter duration of 1-3 months in getting a Proof of Concept approval from banks after a qualified meeting. Proof of Concept approval to Proof of Concept completion stage takes a bit longer and is in the order of 3-6 months. The last stage of converting a Proof of Concept into an actual sale of products, custom solutions or services seems to take the longest and is said to be in the order of 3-9 months.

The Regtech markets directory published in 2017 a white paper that analyzed the Regtech market stated that before the financial crisis fewer than 68 products addressing regulatory needs had been introduced to the market. Rising 135% from 2007-2011 and 158% from 2012-2016, with 68 new products in 2016 alone. KPMG noted in their pace of Fintech Q2 2017 report that: "Regtech

investment and deal volume continued to gain strength in Q2 2017 with a mid-year total of $591 million invested across 60 deals. Regtech investment has already exceeded 2015's annual results and is on pace to surpass 2016's record. Deal volume is also on track to exceed 2014's peak high of 106 deals."

Similarly, CB Insights European Regtech map notes that: "...since 2013, private Regtech companies have raised approximately $4.96B in disclosed equity funding across 585 deals globally. While the US leads in Regtech deals and funding, countries in Europe collectively account for 18% of global Regtech deal share. Europe has been a hotbed for early-stage Regtech start-ups with a focus on solutions for the financial services industry." They go onto predict a total of $1.29bn of new Regtech funding by the end of 2017" (Regtech Markets Directory, 2017: 6) and the global demand for regulatory, compliance and governance software is expected to reach $118.7 billion by 2020 (Medici, 2016).

A Moody's Analytics survey from April 2018, (122 responses from compliance, technology and finance sector professionals) showed that 63.1% of respondents think that the Regtech budget will increase in the next 2-3 years. Also, the Dow Jones / SWIFT Global AML survey showed that 59% of the respondents say technology has improved their anti-money laundering (AML), know- your-customer (KYC) and sanctions requirements (Dow Jones / SWIFT, 2017)

Failure on the part of market participants to adapt to the newer digitalized infrastructure presents a business risk that may separate winners from losers in the coming years. As well, failure to adapt to a more automated regulatory compliance process may leave participants with platforms ill-suited for the current regulatory framework (Armstrong, 2017: 6).

Finally, it will be interesting to see how the cat-and-mouse game between supervisor and supervisees will evolve. Mice will know that thanks to Regtech, cats have improved their ability to detect law breaches. "But there will always be grey areas wherein to test the effective reach of the law" (Enriques, 2017: 8).

3 Conceptual Framework

As covered in the literature review, the story of financial regulation is cyclical. The following in-company project will discuss the implementation of a new electronic communication surveillance solution in a top-tier Financial Institution as a demonstration of commitment to United States regulatory demands.

Electronic communications are of extreme importance for any institution, they can serve as prevention and evidence of risky behavior. Before the 2008 crisis a JP Morgan manager told his employees to stop putting mortgage related stuff in writing, as a package of old, cast-off mortgages with serious issues (about 40% of the borrowers were blatantly lying about their incomes on applications) was packaged and sold as a low-risk security (Business Insider, 2014). Although this was a very wrongful act it serves as example to how this manager was aware that himself and JP Morgan could be traced by communications.

Emails, telephone calls, and electronic chats were a crucial part of the evidence amassed in the LIBOR[6] (London Interbank Offered Rate) investigations and other FX rate fixings worldwide. If the rates are low it means there is confidence in the system and lenders will get their money back. If rates are high it means the whole system maybe on the verge of a meltdown. If determined in an untruthful way, it could be an incentive for lowering the rate to falsely show stability and/or to inflate derivative profits.

This rate is used as a benchmark for determining interest rate for various debt instruments, mortgages, corporate loans, government bonds, credit cards and student loans in various countries. As such, the LIBOR manipulation scandal had big implications "robbing Baltimore and other cities of millions of dollars in returns on investments such as interest-rate swaps" – themselves risky financial instruments that big banks force cities to use in order to fund transit systems, schools, water works, and other city services. (Public Banking Institute, 2012).

For the purposes of understanding this risky behavior a UBS trader in another exchange told his broker via chat: "If you keep 6s (the six-month Japanese Libor rate) unchanged today… I will do one humongous deal with you … Like a 50,000-buck deal, whatever," according to the Zurich-based bank's December 2012 settlement with the regulator. "I need you to keep it as low

[6] LIBOR is the London Interbank offer rate, average of the interest rate that banks are lending to each other.

as possible … if you do that … I'll pay you, you know, 50,000 dollars, 100,000 dollars … whatever you want…" (Bloomberg, 2013).

In 2013 a group of traders were caught manipulating the currency market, basing their efforts around the 16:00 London WM/Reuters currency fix" which determines the rates for different currency pairings. Banks usually make a profit with their client orders by buying a currency in the market at a lower rate than the rate it uses to sell to clients (Whistle-blower security, 2014).

Traders can manipulate this fix rate to make some illegal profits, and in this case, they used chat rooms to share information about impending client order flows (which are usually supposed to be kept confidential) (Whistle-blower security, 2014). Goldman Sachs, Barclays, Deutsche Bank and UBS are now collaborating with the regulators. Calling online chatrooms as "The Bandit's Club" and "The Cartel" and bragging about their fixes within the chats, shows that big banks traders not only poorly behaved, but did it with pride (Forbes, 2015).

Even Bloomberg reporters were participating in multi-firm chatrooms (e.g. Bloomberg chats, ICE chats, Reuters chats) and they are forbidden to participate in client chat rooms on the company's terminal (Bloomberg, 2013).

Michael DuCharme, head of foreign exchange and business growth and development at Seattle-based Russell Investments, which oversees about $246 billion, said in a Nov. 18 interview, before the UBS announcement that it was banning the use of multi-firm and social chat rooms. "If the chat rooms contribute to the collusion, then I think that can be worked around. I don't know if banning that avenue would be sufficient." (Bloomberg, 2013). Which raises a very good question following the ban of multi-firm chatrooms on several institutions following the scandals. Is it really the mean of communication that's at stake or is it a deeper conduct issue, blind profit-seeking nature of employees and employers.

Between 2008 and 2015, 16 traders from at least four major Financial Institutions defrauded the Commodities Exchange (COMEX) gold and silver futures markets mainly by spoofing the markets (tricking the markets into thinking there's more demand than actual). Post-spoof chats show us again, the abusive nature of this behavior: Trader 1, "so glad I could help…got that up 2 bucks… that does show u how easy it is to manipulate so[me]times" (Silver doctors, 2018). The Commodity Futures Trading Commission and the Department of Justice are investigating and charging this case.

Even the blow-up of the Chicago Board Options Exchange (CBOE) Volatility Index (VIX) in February 2018 led to an alleged whistle-blower writing a letter to the SEC through his lawyer alleging the CBOE Volatility Index, a key measure of market fear, is subject to potential manipulation, and that it could be causing nearly $2 billion in annual gains and losses to investors. The Financial Industry Regulation Authority (FINRA) was reportedly looking into alleged manipulation of futures on the VIX and CBOE volatility index, according to The Wall Street Journal (CNBC, 2018).

Below, Figure 2 presents a sample market legislation and the incidents of misconduct 1985 to 2016:

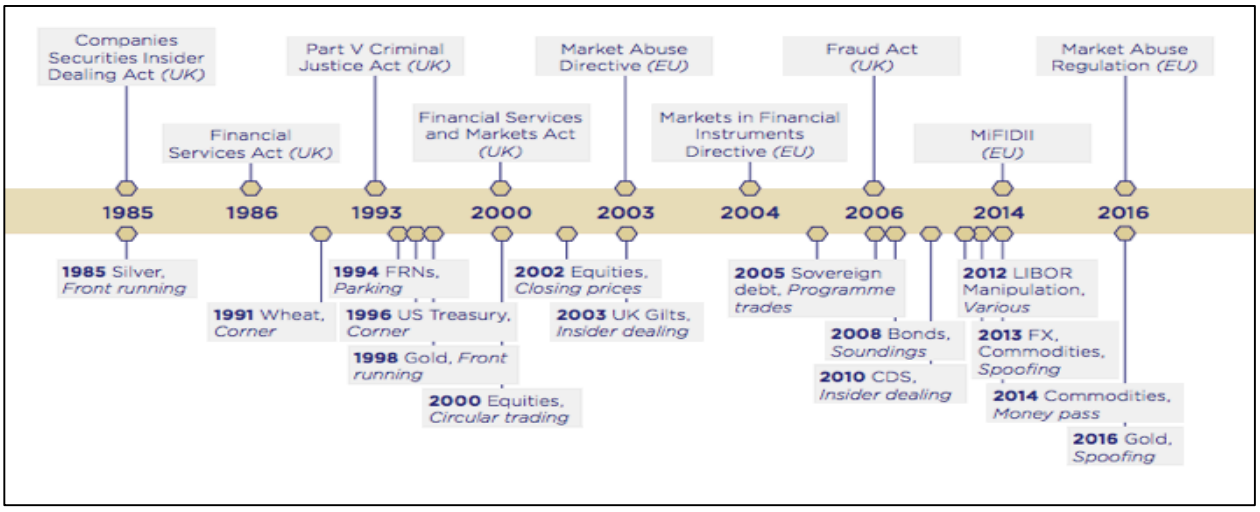

Figure 2: Sample Market Legislation and the Incidents of Misconduct 1985-2016. Source: "FICC Markets Standards Board Annual Report"

As shown manipulation is therefore fundamentally an issue of intent, but how does one prove intent? By noticing unusual trading patterns and crossing them with communications that prove that same intent.

How much could be prevented with the right tools in place is just one of the many questions that regulatory technology tries to tackle.

Technological advances like Cloud Computing, Big Data Analytics, Machine Learning and AI not only allow for lower compliance costs but also for increased efficiency in spotting and processing compliance breaches. Data mining algorithms based on machine learning can organize and analyze large sets of data, even if this data is unstructured and of a low quality, such as sets of e-mails, pdfs and spoken word (IIF, 2016).

The benefits of an advanced surveillance tool can save millions in regulatory fines, and bring clients trust with it. And trust is worth many millions more.

This in-company project will follow a Financial Institution in the area of surveillance and conduct monitoring: such as monitoring traders, registered representatives, employees, and customers for regulatory purposes.

Alvarez and Marsal (2018) report demonstrated that most of the start-up engagements are Proof of Concepts. This in-company project will follow a Proof of Concept before implementation decision, giving an accurate timeline of the duration of the Proof of Concept and the conversion into an actual sales product.

One of the biggest challenges we are going to discuss in this in-company project is reducing the number of false alerts generated by surveillance systems, either by Natural Language Processing, Lexicon based or Anomaly detection. Solutions capable of multi-vector analysis are one of the main objectives when searching for the right surveillance Regtech solution. Programs can be trained with historical data, and be used to detect abnormal patterns and trends.

As stated above the rise of electronic communications scandals in the financial industry has FINRA's attention to how institutions are monitoring and recording them. Just FINRA's fines on electronic communication cases have more than doubled, from $2.7 million in 2008 to $6.2 million in 2015 (Electronic Communications Compliance Survey Report, 2016). The Financial Industry Regulation Authority is a self-regulatory organization of the securities industry, it's not a regulator, but its powerful and important for the industry. The Series 24 License provided by FINRA also known as the general securities principal, allows the holder to supervise many areas of an investment bank and grants the responsibility to review communications of associated persons[7] (FINRA Rule 1011), this is important to understand the concept of Supervisor during this in-company project.

[7] The term "Associated Person" means: (1) a natural person registered under NASD Rules; or (2) a sole proprietor, or any partner, officer, director, branch manager of the Applicant, or any person occupying a similar status or performing similar functions; (3) any company, government or political subdivision or agency or instrumentality of a government controlled by or controlling the Applicant; (4) any employee of the Applicant, except any person whose functions are solely clerical or ministerial; (5) any person directly or indirectly controlling the Applicant whether or not such person is registered or exempt from registration under the FINRA By-Laws or NASD Rules; (6) any person engaged in investment banking or securities business controlled directly or indirectly by the Applicant whether such person is registered or exempt from registration under the FINRA By-Laws or NASD Rules; or (7) any person who will be or is anticipated to be a person described in (1) through (6) above.

FINRA itself has deployed cloud storage and computing, big data analytics, machine learning and natural language processing to enhance its market surveillance and other regulatory functions (FINRA, 2018). Nevertheless, while FINRA is aware of limitations (e.g. number of false alerts in surveillance systems) its rules require firms to maintain reasonable supervisory policies and procedures related to supervisory control systems in accordance (e.g. FINRA Rules 3110 and 3120) (FINRA, 2018). This includes having reasonable procedures and control systems in place for supervision and governance of Regtech tools, including supervision of AI-based tools and systems (FINRA, 2018).

Computer programs trained with historical data may in fact be used to look for suspicious patterns and trends in current data, or identify future patterns and trends. But to be really effective the institutions lines of defense as defined in the literature review, need to coordinate efforts. In the case of electronic communications, the 1st Line of Defense is responsible for identifying the issue whereas the 2nd Line of Defense is also responsible for leading the escalation process that follows. They each have specificities which we will follow in the in-company project.

Finally, this in-company project will follow the decision between several Regtech outsourced tailored solutions and its implementation concluding on how it can help preventing risky behavior and improve overall regulatory compliance.

4 In-Company Project

This case serves as an example of how *Players* can benefit from cutting edge regulatory technology solutions, with focus on electronic communications surveillance and review process in the United States.

As previously discussed Regtech solutions apply core technologies with lower-cost models to people and processes that disrupt legacy approaches. The impact includes a reduction in costs, improved regulatory effectiveness and better revenue generation, customer engagement and capital allocation (Alvarez and Marsal, 2018).

Electronic communications had a significant role in most of the risky behavior cases in recent years. And the transcripts from these cases serve to demonstrate that many risks could be prevented with the proper surveillance system in place.

In the United States, Front-Office Supervisors are required to be the first line of defense against "bad actors" protecting *Players* from market abuse charges, misuse of client information, front running[8], spoofing, etc. To illustrate how complex regulatory demands can be, below are some of the regulations governing electronic compliance:

- SEC Rules 17a3 and 17a4 of the Securities and Exchange Act of 1934;
- FINRA Rules 2210 and 2212-2216;
- FINRA Rules 3110, 3120, 3150, and 3170;
- SEC Rules 204-2 and 206(4)-7 of the Investment Advisers Act of 1940;
- FINRA 4511;
- FINRA 4513;
- FINRA Regulatory Notices 07-59, 10-06, 10-59, 1139 and 12-29;
- January 2012 SEC National Examination Risk Alert (Social Media);
- SEC Guidance Update – Guidance of the Testimonial Rule and Social Media (March 2014);
- CFTC – Clarification of NFA Compliance Rule 2-10(a) and CFTC

8 Entering into an equity trade options or futures contracts with advance knowledge of a block transaction that will influence the price of the underlying security to capitalize on the trade.

Regulations 1.35(a).

The challenge for Front-Office Supervisors is finding the proverbial "needle in a haystack" – the combination of Email, Chats, transactions records, voice logs and other reports – that should be flagged for suspicious activity, and reviewed in conjunction with Compliance and Anti-Fraud teams.

To appropriately address the nature of these threats, holistic risk assessment tools that gather these records (Email, Chat, Voice, Trade Logs, Human Resource Files, building entry records, expense filings, etc.), discover correlations, and provide a credible output that necessitates supervisory review are of extreme importance.

In order to meet United States regulatory objectives, *Player1* as we will describe for confidentiality purposes, sought from 2015 to enhance electronic communications surveillance processes by meeting with several vendors specialized in electronic communications and holistic surveillance.

Banks and other institutions are paying out billions of dollars in fines, penalties, and settlements for misconduct and fraud situations. In an effort to prevent this abuse, the US regulators are focused on making sure firms have the appropriate supervisory tools to support a strong ethical and compliant culture. The tools are part of the first line of defense for effective governance, risk management, and internal control.

Upon identifying the risks described and meeting with the regulators to address them, *Player1* considered a new surveillance solution to be implemented as a replacement for the current solution in place, one that increases the quality the electronic communication control and review, as well as integration of other and new regulatory requirements (multi-vector analysis).

The initial step is to define the business requirements, what do we want to implement? What would be ideal in a utopian context? The first objective is then to maximize business needs.

The next step is submitting the business requirement document and meeting with commercial teams of vendors to review each requirement and to clearly state their roadmap to address the current issues. They need to perform exhaustiveness checks in points such as Cybersecurity (to prevent possible leaks of information), business continuity plans, dedicated on-boarding teams (…).

Also, meeting with other *Players* in the market makes up for a very important part of choosing the right Proof of Concept and consequent solutions. This in-company project addresses all the meeting minutes and summarizes the key takeaways.

Minutious decisions and approval committees evaluate all the possible solutions, gathering feedbacks from the key stakeholders. Upon that, one solution in chosen to perform a Proof of Concept, which will be described taking into account all the confidentiality issues that such a project incurs.

In this Proof of Concept, what we will describe as *Solution1* (company specialized in security analytics) for confidentiality reasons, is evaluated as a tool to detect insider threats and improve the supervisory review process for electronic communications. Continuous surveys and feedback are gathered from all the teams involved. Again, this in-company project addresses all the meeting minutes and summarizes the key takeaways.

The tools utilized for supervisory review must be efficient and effective for the supervisors performing the review process. In addition, they need to be able to identify, analyze and manage risks in the organization with a reasonable level of confidence. The current tool used for electronics communications review which we will describe as *LegacySolution* (multinational software company) for confidentiality purposes, is no longer effective given the large volume of flagged messages, lack of quality alerts in consideration of regulatory expectations.

Within the electronic communications surveillance industry there are several techniques to monitor messages for "bad actors", namely: Lexicon based, natural language processing ("NLP"), and anomaly detection.

Each one of these techniques has Pros and Cons:

Lexicon based: Useful when the content being reviewed has a high degree of subject matter expertise content (e.g., trader lingo, specialized execution dialogue, chat rooms, etc.) which are well suited for search-based technique to flag conversations where sensitive trigger words or short phrases are used.

Natural Language Processing: Valuable when reviewing communications involving full sentences. This method relies on using an initial sentence data set to train the NLP system as a means to flag similar sentences for review.

Anomaly Detection: These are techniques that rank the frequency of occurrence for certain words and phrases to establish baseline patterns and trends. Surveillance is then focused on flagging uncommon words, phrases that suddenly start to trend or break establish patterns.

Each of the above techniques presents trade-offs for deployment in a trading floor environment, requiring some upfront investment and ongoing monitoring: building and maintaining a set of lexicon libraries or natural language processing training data sets and monitoring of their ongoing performance. An ideal system might incorporate all three practices within their toolkit.

Lexicon based techniques are particularly effective in trading environments which naturally contain high usage of chats, subject matter expert discussion with specialized lingo – particularly sales/trading related language: collusion, trade manipulation, information asymmetry, etc. Consequently, U.S. regulators are very comfortable with the application of these techniques, since the vast majority of banks use these in their surveillance today reality.

The following chapters will review and follow the Proof of Concept process, describing its results and implementation, providing an inside look at the increasing demand for new regulatory technological solutions, as well as their benefits and issues.

The research questions for this in-company project will be:

- Can Solution1 help in reducing the cost of surveillance?
- Can Solution1 successfully identify the employees that are putting the company at risk?
- Can Solution1 allow for a quick response to the regulators?

5 Analysis of the Information

Conduct and Ethics are part of *Player1* core values. In order to support those efforts and be pro-active in detecting abuse, *Player1* is focused on making sure the appropriate supervisory tools are in place. These efforts are also in line with the regulatory expectations in this control segment. These aspects are the primary drivers for the Front-office search of tools that better provide effectiveness governance, risk management, and internal control.

5.1 Business Requirements

Defining the business requirements is the first step in choosing the appropriate solution. *Player1* is looking for a tool that can ingest electronic communications with a satisfactory workflow.

A tool that accepts foreign language lexicons, allows for reporting capabilities and proper audit trail. This system should be ready for segregation of duties (1st Line of Defense VS 2nd Line of Defense).

Regulatory requirements are increasing and so is the need for a holistic surveillance solution that delivers full visibility into user behaviors, timely and relevant insider risk insights through advance analytics, and actionable intelligence upon which an effective and efficient surveillance program can be established.

5.2 Meeting with other *Players*

Defining our assumptions is important, but understanding what our competitors are doing and if they share the same assumptions is as important. *Players* with similar dimensions all face the same regulatory pressures and how they choose to react is a good benchmark for any relevant decision in the sector.

As discussed in the literature review, most Regtechs have only done Proof of Concepts with banks, from one to multiple implementations. The typical institution uses fragmented legacy technologies and data sources. As such, the integration of siloed infrastructures can become a bottleneck in the on-boarding process.

Financial Institutions are still mostly unfamiliar with the reliability and acceptance of new Regtech solutions, therefore sharing experiences and approaches is crucial for the development of the sector.

For confidentiality reasons, I will address the other *Players* as *Player2* and *Player3*. And the solutions will follow the same logic for the remainder of the paper.

Player2 tested *Solution1* (company specialized in security analytics), *Solution2* (company specialized in cognitive computer services) and *Solution3* (company specialized in overall big data analytics) and their determination was that *Solution1* was better suited for use in surveilling a trading floor environment, as it was quicker to flag relevant content (sales/trader lingo in

chats/emails), versus having to train the Natural Language Processing model to identify similar instances.

Player2 implemented *Solution1* for electronic communications surveillance and *Solution3* for trade surveillance monitoring around 3000 employees. Which we argue it's not the ideal, through this in-company project we defend the implementation of a holistic multi-vector surveillance tool that allows for integrated analysis.

Player2 feedback on *Solution1* lexicon design and library creation was positive in that it was an intuitive process which was designed for end user customization, allowing for the sharing of lexicons and for each Supervisor being able to create a bespoke lexicon.

As a result, Player2 has a small *Solution1* IT/ Front-Office Supervision Team supporting a largely decentralized approach to the management of the surveillance tools, putting a great deal of flexibility into the end user´s hands.

In addition, they found *Solution1* forensic capabilities to be a key selling point for audits and investigations.

Player2 was recently fined by Japanese regulators for information leakage across Chinese Walls. Specifically, an Equity Analyst with temporary exposure to material non-public information (during a specific reporting window) was sharing information with sales and traders on the distribution side. The internal investigation to identify communications that were occurring during a restricted time window was conducted through the use of *Solution1* forensics and symbol lexicons.

Player1 also, sought feedback from *Player3* on their *Solution2* deployment, sponsored by their Compliance surveillance.

Player3 tested *Solution2* and then proceeded to deploy. The topic was discussed while they were still in the testing phase (e.g. end user deployment had not started yet).

Player3 determination to choose *Solution2* to monitor around 5000 employees to start with, was based on their view that could be used across the organization: Investment Banking Capital Markets Trading and Sales, Wealth Management, etc.

Player3 created a central team to train the natural language processing models for each desk/team, they determined that the training data sets would not work across the entire organization and instead implemented customized training sets for each role. *Player3* feedback was focused on

the significant time commitment necessary to adequately train the natural language processing in order to achieve satisfactory results.

The natural language processing model tuning is time consuming and requires close management from dedicated staff.

As a result, *Player3* is operating with a fairly large IT/Compliance and electronic communications surveillance teams implying a largely centralized approach to management of the surveillance tools, with supervisors reviewing the output.

Player3 plans to run *LegacySolution* and *Solution2* in parallel for an undetermined period of time to become comfortable with the output, explain the toolkit to their regulators and await their feedback on whether these controls are satisfactory.

While evaluating new supervisory controls, and gathering feedback from a group of Chief Control Officers in the industry, it is clear that the best way to identify "bad actors" is to take a holist approach to their activities.

This means using multiple vectors (e.g., email, chat, building entry logs, trade exceptions, etc.) within the same system, instead of the current siloed approach were trade surveillance, fraud detection and electronic communications reviews are run separately) to detect cases of market manipulation, insider trading, data exfiltration and conduct risk.

This siloed approach relies on the Supervisor alone to connect and identify aberrant trends across all vectors.

Using a single system to apply a comprehensive multiple vector analysis approach brings surveillance and supervision to the next level and closer to regulators´ expectations.

5.3 Meetings with Vendors

All Regtech providers focus on advanced technology to solve compliance issues, however choosing the right Regtech partner requires a forward-looking strategy. *Players* needs to reflect on the pros and cons of each solution that appears to align with the technological roadmap of the business requirements. Compatibility with existing systems and a deep understanding of the business is critical for the stability, sustainability and scalability of the solutions.

Player1 is considering between *Solution1* and *Solution2*. Below are the key takeaways from the meetings with the vendors.

The meetings with *Solution1* vendors resulted in the following takeaways:

- *Solution1* can ingest multiple data feeds (e.g. electronic communications, trading activity, building access data, material non-public information, restricted list information, regular business hours per desk, etc.);
- Can provide behavioral analytics and customized alerts based on all the data feeds listed above. The tool can be configured in order to perform cross data analysis, identifying the "normal" pattern per user and then highlighting deviations;
- Specific alerts can be put in place for: multi-firm chatroom detection, public/private side communications, off-hour alerts, trade alert detection;
- Implements a risk scoring model, with all alerts described above given a weighted risk score that can be combined if several alerts are triggered for the same event;
- Can ingest live data streams to allow intra-day (T-0) monitoring.

Overall, *Solution1* has a credible offering that will allow for a more holistic review of trading floor activities.

Moreover, *Solution1* could be the answer to perform the following trade surveillance controls:

- Large barrier-options[9] surveillance;
- Large Orders;
- Out of Hours activity;
- Multi-dealer chats;
- Restrict client data visibility based on lexicon;
- Communications between sales and traders;
- Margin /mark-up controls;
- Fix manipulation;
- Communications around non-disclosure agreements.

The meetings with Solution2 vendors resulted in the following takeaways:

9 Type of derivative where the payoff depends on whether or not the underlying asset has reached or exceeded a predetermined price.

- Partnership with *USExchange* (confidentiality purposes) to integrate the electronic communications surveillance and trade surveillance and allow for the cross flagging of events. The capabilities were still in design and not available to test;
- Does not present a strategic approach for multi-vector analysis – to systematically embed other sources of structured and unstructured data in their review tool;
- Does not offer the same multi-vector capabilities as other vendors and there is no minimum viable product available to review from their partnership with *USExchange*.

To successfully implement a holistic surveillance framework the vendor selected, besides proving a software product, must provide data scientists and deployment staff.

Implementation requires clean data ingests, iterating on important product customization and enhancements, and importantly data analysis to ensure we are getting maximum output from the tools.

Furthermore, once the electronic communications are ingested, there are new analytics to be designed, tested and applied to this data trove – either for surveillance enhancements or for purely commercial purposes (e.g. Sentiment Analysis).

Over the course of many interactions with *Solution1* and *Solution2* it was concluded that Solution1 will interact with Player1 via their Head of Sales and Chief Operating Officer, and when asked probing questions on product capabilities *Player1* has consistently been exposed to their technical design team.

Solution2, in contrast has interacted via their Head of Sales and Product Marketing, but when probed on technical topics, *Player1* was only exposed to some of their product design staff and for the remainder of the inquiries was restricted to interactions with the Sales Teams.

To highlight this difference when a *Player1* employee asked about methods through which he could access data and run test algorithms to identify useful additional controls the Solution1 the Chief Data Scientist was looped in to respond and provided three different mechanisms by which the employee could test his algorithms and incorporate the results into *Solution1* supervisory front-end.

So far, the conclusion of the comparison between the two solutions was evident, *Solution 1* stands out from *Solution2*. But the technological factor is very important. Both solutions use different approaches to electronic communications review.

One uses a lexicon based approach that has been criticize as relatively simplistic, exhaustive and flagged a decent amount of false positives (messages that don't represent compliance or conduct breaches) but praised because it can be extended, refined, targeted and managed with word proximities and meta checks. Also, it allows for integration of what have been traditionally viewed as different activities e.g. trade and electronic communications surveillance allowing for a multi-vector analysis.

Since U.S. regulatory requirements are such that a supervisor must review relevant communications, and at times if a lexicon flagging approach yields too low of a population for review, the random sampling is applied at the recommendation of Compliance. FINRA on its Regulatory Notice for Supervision of Electronic Communications (2007) advises that members using lexicon-based reviews (those based on sensitive words or phrases, the presence of which may signal problematic communications) of correspondence should utilize an appropriate lexicon, take reasonable security measures to keep the list confidential and periodically evaluate the efficacy of the lexicon, being the alternative a reasonable percentage sampling technique, whereby some percentage of the electronic communications generated by the member is reviewed.

For example, another firm recently on-boarded *Solution2* and the main feedback was that they decided to keep also *LegacySolution* in parallel to meet a minimum of 1% random sample review based on lexicon.

Moreover, it took a lot of time to train the tool before seeing first results.

Indeed, natural language processing solution requires a longer time of tuning based on trends observed. These developments are time consuming and require close management from dedicated staff.

As a result, this *Player* has taken a largely centralized approach, whereas *Player1* takes a distributed approach. For *Player1* it is key that a tool is manageable and intuitive at the desk supervisory level.

Natural language processing logic is not yet a proven approach with the U.S. regulators. A lot of time would be needed to fully document all the turning performed over time to clearly show the filtering logic and process.

Working with lexicons with advance analytics is more manageable and straightforward.

The lexicon based logic is still the ideal way to detect abnormal subject matter expert discussions, particularly trading related language: collusion, trade manipulation.

The natural language processing would be more adapted to regular non-specialized electronic communications. *Solution1* tool would take less time to be configured since it is based on lexicon fine tuning, and results of lexicon customization can be seen instantaneously.

While evaluating new supervisory solutions, it is clear that a proper supervision should perform alone on multiple vectors instead of a siloed architecture. Using cross-vector analytics is bringing supervision to the next level and closer to regulators expectations. As such, *Solution1* tool is meeting this standard and proposes the following cross-vector functionalities and advanced analytics:

- Ingests different types of data feeds (electronic communications, trading activity, Profit & Loss data (P&L), premises access data, material non-public information, restricted list information, regular business hours per desk, …);
- Provides behavioral analytics and customized alerts based on all the data feeds listed above. The tool can be configured in order to perform cross data analysis and improve surveillance. The following alerts could be put in place: multi-firm chatrooms detection, public/private communications, off-hour alerts, off premises trading detection, front running detection;
- Proposes risk-scoring model, all alerts described above would have a weighted risk score and these can be combined if several alerts are triggered for the same event, this can be used in order to display to supervisors only events with a risk score above a pre-defined specific threshold;
- Ingests live stream of data in order to do intra-day monitoring. *Solution1* is ready to accept these feeds, the only exception will be for external chat platforms (Bloomberg, Reuters) for which *Player1* relies on daily batches. This intra-day monitoring will bring a better surveillance for the overall platform.

Solution2 team was not able to demonstrate how advanced analytics as described above could be done within their tool.

Internal capacity is a limiting factor to be able to run multiple Proof of Concepts simultaneously so *Player1* will have a much longer time to delivery versus competitors running Proof of Concepts sequentially.

Here again, another bank has been rolling out *Solution1* for over a year, with positive results now showing. As such, the conclusion for on time to delivery clearly favored *Solution1*.

5.4 Comparing Solutions

Businesses need to understand the value added in any new solution for a firm, technological or not, and the best way to achieve that is comparing pros and cons of present and future states.

Analyzing, what the current/future issues of a firm are and if investments can suppress those issues is a very important step in the decision-making process.

As a result, *LegacySolution* and *Solution1* were exhaustively compared, below are the key takeaways for the electronic communications review current state of *LegacySolution*, which supervisors are using to review messages. *Legacysolution* is a third-party vendor system that supports processes on a day to day basis and modifies the lexicons over time to address issues raised by supervisors

Main issues are:

- It's flagging too many false positive messages and causing the review to become a time-consuming process;
- It's difficult to use, the users have stated the system can be clunky;
- Does not offer context to the emails relative to any other activities, users are looking for the proverbial "needle in a haystack"; It´s difficult to recognize patterns in the emails; Dislocated process with no point of reference;
- Does not offer an intelligent method to: Identify disclaimers; Review disclaimers;
- Lacks controls and review of multi-firm chartroom activity. Unable to review multi-firm chatroom activities. Multi-firm chatrooms like Bloomberg or Intercontinental Exchange chats (ICE) were used as tools to rig interest rate markets in the past as well as other condemning behaviors. Monitoring of these multi-firm chatrooms became a priority for institutions;

- Unable to provide threading of chats or emails, workflow issues when supervisor is present on email;
- At times, a supervisor would encounter a flagged email they need to review but they are present on the communication (the communication is either directed to them or they are carbon copied on it). Supervisors cannot review an email they are present on. Such emails should be approved by the supervisor's supervisor. *LegacySolution* is unable to detect and send such email to the supervisor´s supervisor for review.

On the other hand, *Solution1* is a specialized data analytics provider in the field on internal threat detection. The tool is to be used in order to improve and take full advantage of existing alerts feeds while enriching with all forms of communications and trades data, a tool that:

- Automates and improves on brute-force email review;
- Reshapes siloed trade and email review team workflows by leveraging cross-model analytics and automation.

Solution1 software proposes aggregation, content consumption, visualization & workflow functionalities.

With regards to the main issues with *LegacySolution* and electronic communications review process, Player1 is looking for Solution1 to provide a solution that will remedy such issues.

5.5 Front-end Demonstration

This sub-section serves to give a brief overview of the tool in order to guide the reader trough the Proof of Concept and consequent functional and technical evaluation with non-confidential dummy data.

Login into the tool automatically opens the Explore Page which provides the user with a deep view of events (see Figure 3).

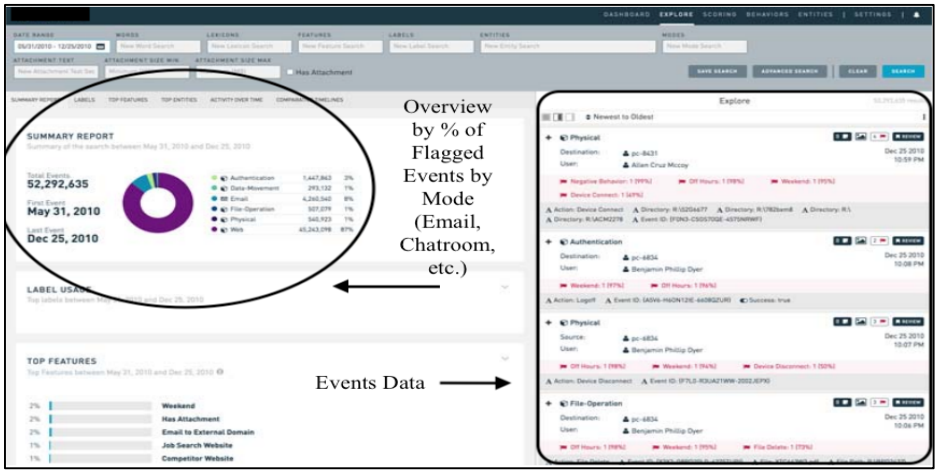

Figure 3: Solution1 Login Page Breakdown. Source: Solution1.

This view is broken down into several sub-views: event viewer, search and summary report (see Figure 4).

Figure 4: Solution1 Events Breakdown. Source: Solution1.

Events data include, entities and roles, probability scores, attachments, timestamp, etc.

The red icon displays the event feature that scored the event. A feature is for example inside information. Each specific feature contains a set of lexicons in accordance.

For each flagged event, the red icon displays the event feature that scored the event. A feature is for example inside information. Each specific feature contains a set of lexicons in accordance (see Figure 5).

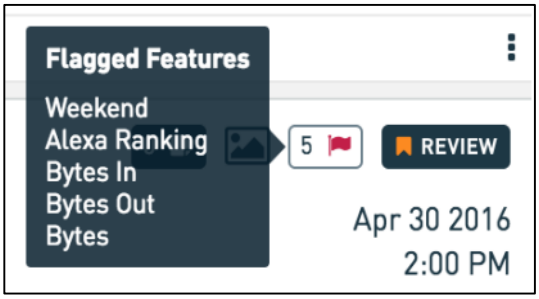

Figure 5: Flagged Features. Source: Solution1.

Upon clicking review the user can choose one of the options below, in order to review or flag it for further review (see Figure 6).

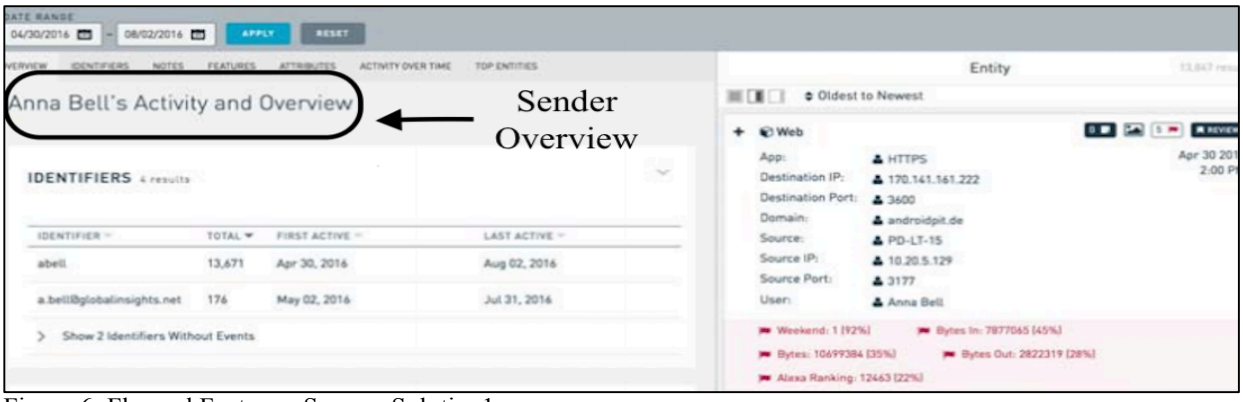

Figure 6: Flagged Features. Source: Solution1.

The Entity Details page provides details and activity surrounding specific senders, recipients, rooms or company participants (see Figure 7).

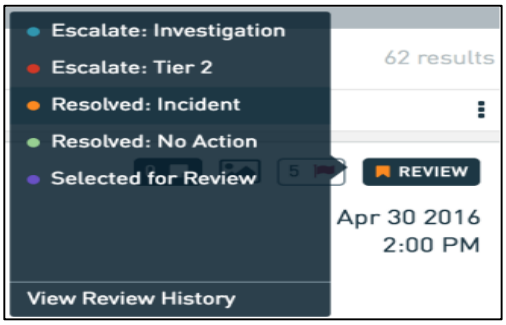

Figure 7: Entity Details. Source: Solution1.

Among other functionalities the user can access specific analytics like activity over time (see Figure 8) or an overall analytics dashboard with key visualizations providing each user with

risk scoring models that make up for an overall behavior scenario, giving an overview of the specific features that triggered on a daily basis (see Figure 9).

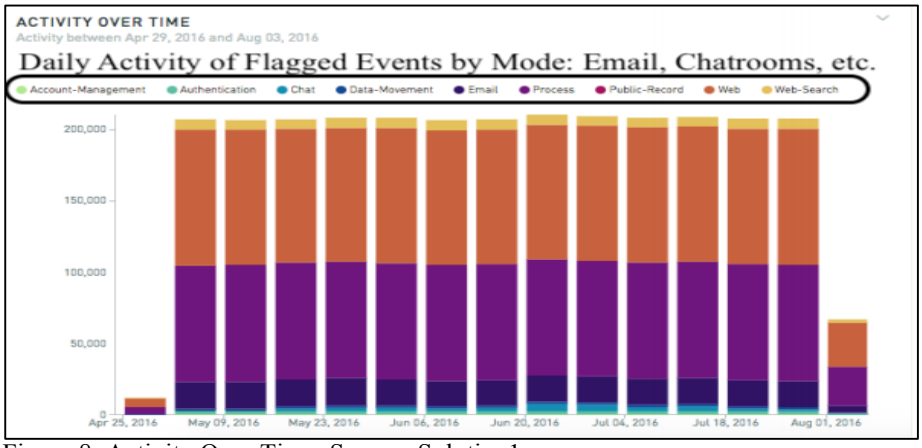

Figure 8: Activity Over Time. Source: Solution1.

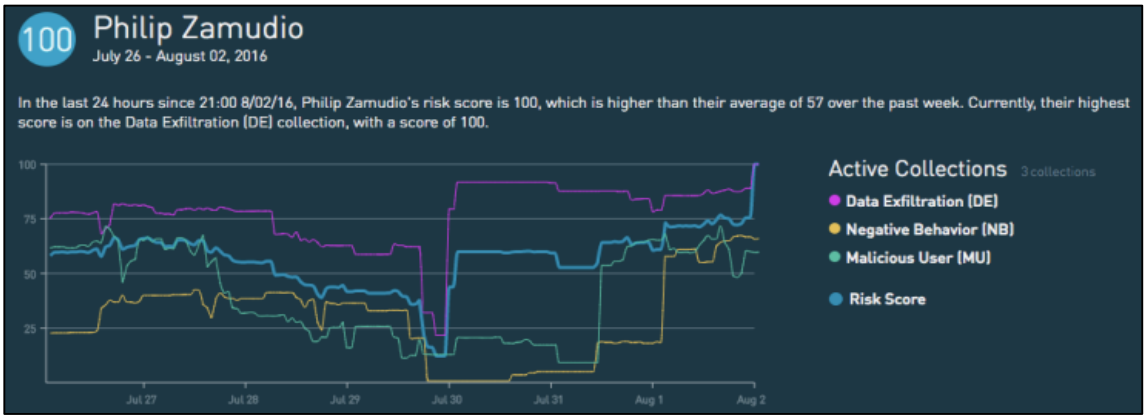

Figure 9: Analytics Dashboard. Source: Solution1.

To end this brief introduction the My Reviews tab, that log the reviewer's historical analysis for triggered events. Which displays events considered for escalation (see Figure 10).

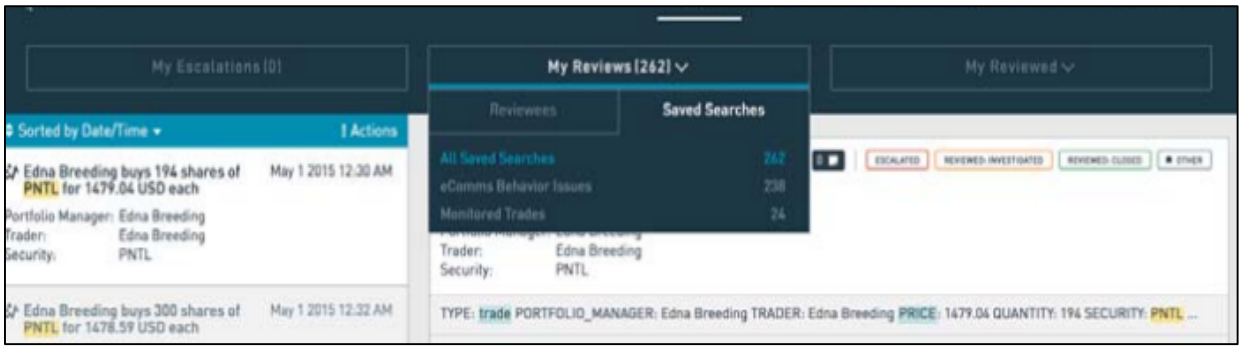

Figure 10: My Reviews Tab. Source: Solution1.

And the Front-end Configuration that allows to configure lexicons (words, domains and even sentiment) (see Figure 11).

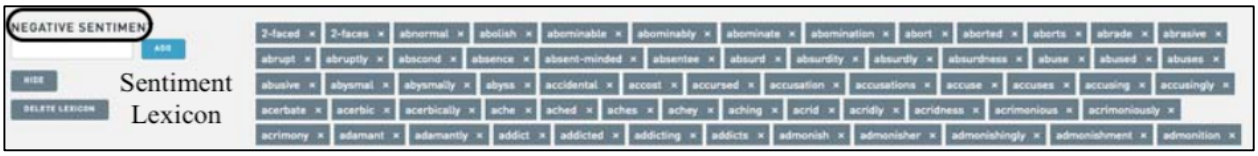

Figure 11: Lexicons Tab. Source: Solution1.

5.6 Setting Expectations

Setting clear expectations without ambiguity is essential to fulfil technical requirements and ensure successful implementations. Although both internally and externally expectations should be revisited, it's imperative to align strategies from the start.

Player1 is looking for a centralized supervisory tool in order for supervisors to perform their daily/weekly/monthly controls is a single location. *Player1* supervisors should be able to have a clear view on desk activity trough this tool.

The ultimate goal is to provide *Player1* supervisors with a new supervisory control framework that would be an improvement compared to our current decentralized state.

For this Proof of Concept, *Player1* expects this tool to be able to analyze all the following vectors in isolation, as well as together, and provide solutions for the current issues that *Player1* faces with electronic communications:

- Reducing the large number of false positives;
- Clunky nature of current review process;
- Lack of context in the current state being unable to relate other sources of data with Electronic Communications review;
- Lack of controls and review of multi-dealer chatrooms;
- Lack of threading of chats and emails;
- Intelligent method to deal with self-review emails.

Player1 main barriers in searching for a new solution are the following:

- The know-your-vendor is extremely long for Regtech;

- A Proof of Concept takes a long time to run (defining scope, extracting data, running and training the tool, involving Compliance, Legal and IT departments in order to get the proper authorizations);
- Long staging of test environment (remote access issues).

Taking into account all the described above, *Player1* took the decision to restrict the Proof of Concept with *Solution1* on electronic communications workflow process only.

5.7 Proof of Concept Conduction

To achieve the goals of the proof of concept, a dedicated environment was established within *Player1* core infrastructure. Over 1.5 million emails and chat messages were extracted from *LegacySolution* for ingestion into the Proof of Concept architecture that was built based on *Player1* specifications.

After the data ingestion and configurations, participants were able to connect to the web based user interface to review the alerts that were generated by the application. The scope of messages for the Proof of Concept consist in: emails, Lync chats, Bloomberg chats, ICE (Intercontinental Exchange) chats and Reuters chats. An IT team performed a preliminary technical review on *Player1* to identify red flags.

Formal governance is designed to ensure the Proof of Concept was aligned with the objectives of the business. The Proof of concept consists in testers from the following teams: Desk Supervision, Business Supervision, Compliance Surveillance and Anti-Fraud. A steering committee meets weekly to review progress of the Proof of Concept.

Since the initial phases of the project, *Player1* coordinated locally and globally in order to socialize Solution1. This was done by providing demos, collecting usability feedbacks and requirements.

The scope of employees includes traders and sales that were monitored in the Front-Office from Foreign Exchange, Commodities and Equity businesses in the U.S. and Brazil. Data included lexicons and electronic-communications in English, Portuguese and Spanish. The lexicons were newly created for the Proof of Concept.

Solution1 will deploy lexicon and analytics features to surface communications involving the following use cases:

- Conduct Risk – Identifying individuals whose communications and behaviors suggest the possibility of harassment of co-workers, evading company oversight, sharing confidential credentials internally or general job dissatisfaction with intent to leave;
- Data Exfiltration – Identifying communications and behaviors that indicate attempts to distribute confidential data to outside parties;
- Market Manipulation – Identifying communications and behaviors that indicate possibility of intent to inflate or deflate the true sales volume, demand, and ultimately, price of a security/asset;
- Insider Trading – Identifying communications and behaviors that indicate the possibility of intent to manipulate the price of a security and/or trading by individuals with access to non-public information about the company.

Even though the proof of concept will just focus on communications, below is an example of the future state of the solution in regard to multi-vector analysis for market manipulation:

Trades FX Rate Fixing / LIBOR Rate Fixing

Monitoring trades for indicators of FX rate fixing, this including identifying:

- Trades with unusually high quantity traded;
- Trades in close proximity to announcements of rates;
- Traders with a high daily value of P&L;
- Traders who have a low P&L for the month to date.

Communications FX Rate Fixing / LIBOR Rate Fixing

Monitoring communications for indicators of FX rate fixing this including communications:

- In close proximity to announcements of rates;
- Involving discussions of benchmark rates;
- Containing congratulatory language communications;
- Employees discussing oversight evasion;
- Containing insider Trading language.

The system will be configured with the existing Lexicon base with the first step being migrating existing lexicons for the legacy systems for 1st Line of Defense and 2nd Line of Defense, routing flagged messages as per the appropriate group. Also, the system needs to facilitate supervisory workflow by providing review, approve, escalate and comment functionality for trade exceptions flagged by the system. Lexicons need to be tuned with feedbacks from various stakeholders, integrating with appropriate signals (trade alerts) to provide context to flagged items.

5.8 Functional Evaluation

As stated above the Proof of Concept test was done by using lexicons created specifically for this Solution1 project. The comparison between *LegacySolution* and *Solution1* is also subject to this major difference since this new lexicon set is not as exhaustive as the old lexicon. In a production environment *Solution1* would need to be further fine-tuned based on user experience.

During this Proof of Concept, Front-Office Supervisors tested the following functionalities:

- Regular electronic communications review (open message, close message, add comment, flag message as "pending", send a comment to another person);
- Use "show context" functionality to get more background around a specific time period;
- Use of pre-defined search functionalities (targeted searches on specific employees, detect multi-firm chatrooms, capture bilateral chats between targeted employees, and search for case sensitive keywords);
- Use of Solution1 Query Language for highly specific search results (<Field>:(<Qualifier> <Operator> <Value>)). This is used to query Solution1 database directly, this can be used to do sophisticated searches (e.g. looking for bilateral chats between two different business units considering also a specific pre-defined time range).

The Front-Office Supervisors and Compliance feedback was that *Solution1* successfully applied smart logic to remove noise, demonstrating the capability to remove thousands of messages which were being flagged due to disclaimers in *LegacySolution*. *Solution1* can also use

a whitelist function in order to detect which senders should not be flagged due to specific reasons: robots sending automatic emails, internal blast emails. Which also represents a great opportunity to remove noise.

Another very positive aspect is being highly configurable, and that is crucial to make sure the system can evolve at the same time as regulatory requirements. During the Proof of Concept period, several requests/upgrades were requested. These were implemented very quickly. For example, *Solution1* was able to roll out a new template of their review dashboard during Proof of Concept period, this update went smoothly without issues for any tester. Moreover, new lexicons were implemented in foreign language (Spanish, Portuguese) in order to monitor Latin America messages, again this was setup very quickly.

Solution1 system proposes a workflow process in order for users to share with a dedicated support team and tool that allows disclaimer management. It maintains a database of disclaimers which should not be flagged by the system. This is important to improve the overall quality of the system alerts going forward. The escalation process is intuitive, moreover users can attach a message to a flagged message. Also, *Player1* would have direct access to the database in order to connect it with its own Analytic tools in addition to *Solution1* built-in analytics.

Solution1 appears to be a viable replacement to *LegacySolution* as it possesses many features which are currently lacking: the ability to create saved searches, the consolidation of email threads, suppression of disclaimer language, showing the policy (e.g. inside information) for which the message was flagged, highlighting text that precipitated flagging and the ability to submit certain messages for future exclusion. Once a full training on the system is provided, the navigation is easy enough.

Solution1 offers the opportunity to define a specific Compliance Surveillance lexicon. These messages would be only accessible to Compliance. *LegacySolution* could not offer this fundamental functionality to segregate the 1st and 2nd Line of Defense. This will be a significant progress for Electronic Communications surveillance. By default, *Solution1* offers regular search capabilities, nevertheless the system offers the opportunity to build custom searches with a specific query language and *Solution1* is also working on a way for users to configure their own customized searches.

The negative aspects for the Front-Office Supervisors start with *Solution1* not supporting Internet Explorer at the time of the Proof of Concept. This is a major constraint being that Internet

Explorer is the official browser for *Player1*. According to *Solution1* team, the compatibility with Internet Explorer should be ready at the time of deployment. This would be a requirement in order to officially move to production. Reporting functionality must be improved and developed in order to demonstrate how supervisors are completing their review (backlog aging, review statistics, escalation reports, etc.).

To do targeted searches, the user must know the specific query language that Solution1 offers and write it in the advanced search. It's not easily accessible to everyone. Training needs to be provided. *Solution1* also proposes a user guide in order to perform customized searches. At the same time, *Solution1* is working on a better solution in order to extent search functionalities. Some dedicated employees can be the key contacts in order to help the creation and functionalities in *Solution1* tool (advanced searches, new types of alerts, supervisory mapping management…).

The system could be more intuitive. *Solution1* granted access to its new environment during this Proof of Concept, a great improvement on the interface display was noticed. Some investigation features e.g. wildcards or a simple advanced search are neither non-existent or still very basic and not innovative (in order to search for two individuals that used two or more specific keywords, a specific language query string needs to be inserted and altered).

The Front-Office Supervisors concluded that *Solution1* is less mature than *LegacySolution* with minor bugs and displayed issues during the test. But most of these issues were corrected during the testing phase, successfully demonstrating *Solution1* reactiveness. *Solution1* has a detailed IT developments roadmap in order to develop alerts quality and improve user experience.

But even if *Solution1* pondering the pros and cons, showed its ability to customize the interface quickly and improve noise reduction, some areas for improvement were noted during the testing phase.

The user interface improved during the Proof of Concept, *Solution1* proposed an IT roadmap that include several improvements on user interface, *Player1* feels comfortable that the upcoming updates will improve the overall user experience.

The tool lacks reporting functionalities, and this is core for a surveillance tool, since *Player1* needs to demonstrate to regulators how timely backlogs are being reviewed, how many messages are being escalated and how many hits are flagged per lexicon. Reporting capabilities are part of *Player1's* requirements.

Users need to be trained on the specific query language, as its important for complex searches. With the creation of a center of competence this should be achieved. The disclaimer process will also need to be further developed in order to become automatic. The tool is supposed to highlight flagged keywords in attachments, the test was not conclusive for this functionality and the issue was communicated to *Solution1* which replied that the issue was going to be fixed in production. Also, the export functionality was not working at the time of testing, again the issue was communicated and should be fixed in production.

It's not easy for users to scroll quickly through flagged messages to focus on the most sensitive ones. The snippets or flagged keywords are not displayed in the scrolling window, so the user needs to open each message in order to see what was flagged. The system didn´t have natural langue processing capabilities at the time, it was based on lexicon hits. It would bring value to slowly incorporate natural language processing and sentiment analysis to flag messages based on the sender mood.

Some messages are flagged for non-obvious reasons. Non-sensitive words were flagged by the system while they should not have. Solution1's team is aware of this issue and working to fix it.

5.9 Technical Evaluation

IT Security evaluated Solution1 and concluded that it's catered to *Player1* needs being that Vendor Support is available and it allows for integration with the in-house applications.

A vendor review was performed and classified by risk level:

Risk High – Last third-party audit was completed two years ago. *Solution1* will commit to a semi-annual penetration testing;

Risk Medium – No security awareness program in place. *Solution1* will start to have a security awareness program from now on;

Risk Medium – No automated security code scanning tools are run on the entire code prior to each release. *Solution1* plans to have a code scanning (application security testing) in place by the standard development process;

Risk Medium – No software security training for developers, *Solution1* plans to engage an external training resource to provide Secure Software Development training;

Risk Medium – Security experts are not included in development process. *Solution1* focus to date has been to secure the infrastructure that hosts *Player1's* data and services and leverage secure frameworks to build the platform;

Risk Low - No annual acknowledgement of Non-Disclosure Agreement or code of ethics. *Solution1* one will have in place both.

IT application support also provided an overall feedback about the tool focusing on user interface, performance and usability.

For the user interface the positive aspects were the general design and the clean interface with standardized views nevertheless some views were busy with too much detail.

For the performance, the search functionality was very fast and configurations could be applied on the fly without reloading underlying data with lexicon adjustments also being done in real time. Although some historical information was not observed.

For the usability, the navigation was quick and responsive and it's a very useful for a user versed in advanced analytics. Nevertheless, it requires training to understand some no that intuitive aspects like proprietary query language searching.

The overall impression from the technical evaluation was that *Solution1* is a robust electronic communications surveillance tool with advanced analytics and scalable underlying technology (e.g. elastic search[10]).

5.10 Cost Analysis

Another very important step in the decision process is the cost analysis. For confidentiality purposes values cannot be addressed, but the factors for ponderation are the following:

Internal Costs – Governance approval process and dedicated internal team support e.g. IT Application Security and Support teams;

Phase 1 (Implementation) – Infrastructure servers with an initial estimated data size of several Terabytes and setup costs. Also, a Professional services fee that represents almost two thousand hours of work across the different service roles;

[10] Powerful analytics tools that allow for a very fast search through big data.

Beyond Phase 1 – Annual cost for technical lead, Operation Engineer, Field Data Scientist and Annual subscription license fees for each monitored user. Depending on the number of users which will be in the thousands, *Solution1* can provide batch discounts.

The conclusion for the cost-analysis was satisfactory taking into account the surveillance potential of *Solution1*.

5.11 Proof of Concept Conclusion

Solution1 tool demonstrated its ability to flag messages based on pre-defined lexicons, so the smart logic was successfully applied to remove thousands of disclaimers and decrease noise. It also offers many interesting capabilities in order to ingest additional data and perform multi-vector analysis.

The proof of concept clearly demonstrated *Solution1's* benefits that would improve the supervisory framework and bring *Player1* in line with regulatory expectations. The main factors considered in the evaluation are the following:

- *Solution1* is able to reduce false positive alerts with disclaimer detection, threaded email detection and broadcast message detection. These features significantly reduce the false positives in the supervisor's and reviewers message queue enabling them to focus on meaningful alerts (see Figure 12 and Figure 13 below);
- Lexicons can be assigned a risk weighting to prioritize the alerts in the supervisor's queue;
- User can create and save their own customized searches;
- Directs the flagged message to next level of supervision to prevent self-review;
- Front-Office and Compliance are able to maintain their own set of lexicons in *Solution1*. This provides Compliance the ability to conduct their own independent review on the same data sets;
- Lexicons can be created in different languages;
- *Solution1* provides controls for multi-firm chatrooms;
- Users can add context to the alert in the review process;

- Application is highly user configurable, so *Player1* is less dependent on the vendor for day to day support;
- User behavioral analytics to identify anomalies and suspicious activity (considering that *Solution1* could ingest multiple data feeds in order to perform cross data analysis).

Solution1 was therefore chosen to be the next electronic communications surveillance tool for Player1.

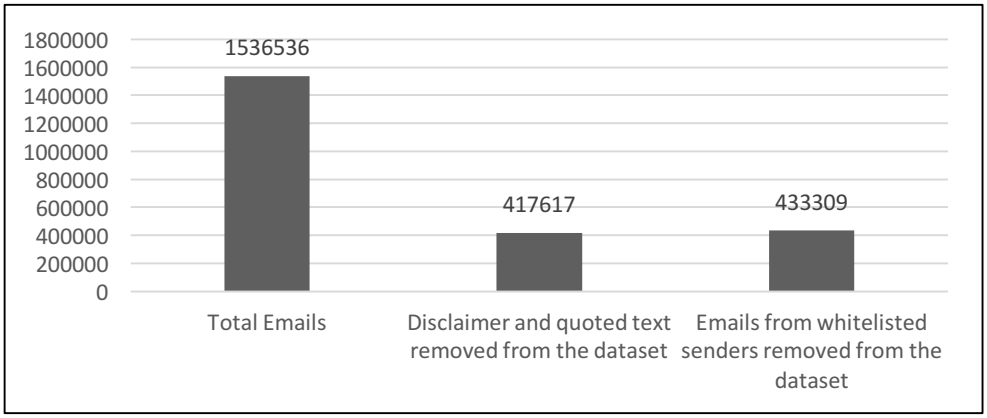

Figure 12: Overall Noise Reduction Solution1 Capabilities. Source: Solution1.

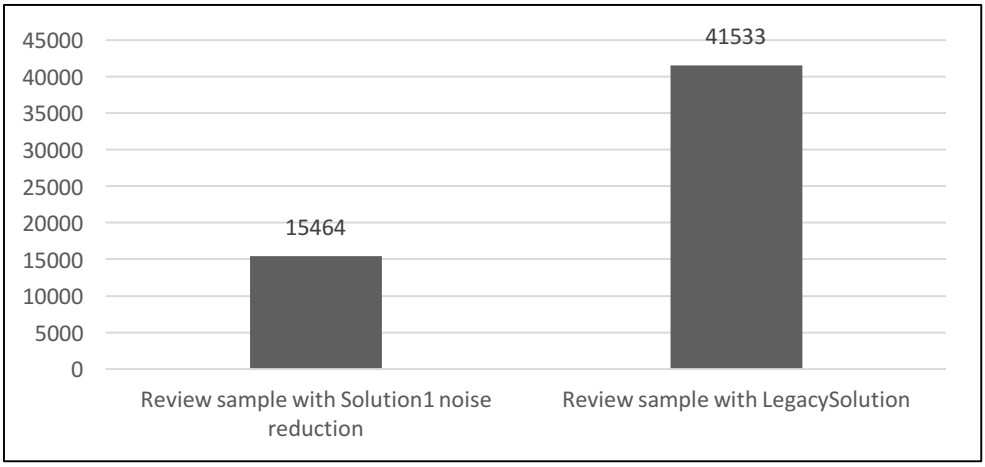

Figure 13: Daily Noise Reduction Solution1 Capabilities. Source: Solution1.

6 Forms of Implementation

As discussed in the literature review, the stage of converting a Proof of Concept into an actual sales, custom solutions or services seems to take the longest out of any stage and its said to be in the order 3-9 months. In our specific case, less than 3 months passed since the Proof of Concept and the implementation.

After board-approvals, architecture and investment committees, the rollout plan is defined and a 100-day implementation program is deployed after a successful Proof of Concept conduction.

For a wider implementation, a phased approach is proposed with the initial deployment focused on a business line and subsequently rolling out to the others. This addresses the immediate needs of the business.

Phase I of the implementation consists in the program preparation and the previewed duration is 5 days. The objectives are: ensuring full alignment on goals, establishing population of monitored users, *Solution1* team on-boarding and development of detailed implementation plan.

Phase II is the actual initial implementation and will benefit significantly from the work done in the Proof of Concept. The previewed duration for this phase is 35 days.

It covers the deployment of the solution and *Player1's* enablement. For deployment, it includes the deployment in User Acceptance Testing (UAT) environment, establishing on-going ingestion for electronic communications, implementation of initial lexicons and analytics on prioritized use cases and in *Player1's* desired workflow. For enablement, the steps are training for business and IT teams supporting the platform and deep dives on day-to-day workflows and use cases.

A program review will be delivered in the end of Phase II, with the success criteria depending on factors such as: deployment of the platform and ingestion of all necessary activity streams, *Player1's* business and technical teams increasing comfort with managing the platform and initial analytics and workflows implemented.

Phase III is the user acceptance testing and refinement, with a previewed duration of 30 days. The objectives for this phase are: deployment of latest release of *Solution1* (releases twice per quarter), implementation of additional/revised analytics and workflow as made possible by latest release and review of operational metrics and tuning of configurations.

The user acceptance testing will identify key users to test initial implementation, and train users 1:1 to understand the benefits and challenges. Fostering their ownership of the program and its consequent success.

Feedback sessions and yet another program review will be performed, being that the success criteria will rely on: key users' acceptance and signing-off initial implementation, comfort and proficiency with the application, business and IT teams capable of supporting business as usual activities to support daily use of the platform, drafting of initial requests for future product evolution (including ranking/prioritization to guide player1 product decisions).

The last Phase is IV, it consists on a final acceptance review and sign-off by User Acceptance Testing users. The previewed duration for this phase is 30 days and the objective is to continue monitoring operational metrics and evolve processes as necessary to drive efficiency and knowledge sharing.

In the end of the 100-day program *Player1* should: transition their target traders to surveillance using the platform, be managing effectively Business as Usual platform maintenance and actively engaging with *Solution1's* community.

Throughout the 100-day program it will be critical that *Player1* and *Solution1* collaborate and share knowledge fully leveraging the content to drive context and precision in analytics.

The focus on end users making them efficient and effective for a successful development and refinement is essential for high performance monitoring and investigation workflows.

7 In-Company Project Conclusion

As mentioned above, enough information was collected from other *Players*, the various vendors and the Proof of Concept, to be able to understand the trade-offs between the product in order to make a confident decision. *Solution1* has a more robust information set than other vendors.

Based on that, *Solution1* was selected for deployment as *Player1's* Front-Office Surveillance tool offering the following benefits:

- Known technology (lexicon based search) which Front-Office, Compliance and regulators are comfortable with and extremely suited for a trading floor environment and its specific lingo;
- Enhances lexicon based flagged communications and improves usability with message threading, disclaimer removal and automatic detection of blast emails;
- Allows for ingestion of multiple risk vectors (e.g. email, chat, trade logs, building entry logs…) to enable the holistic supervision to staff (e.g. off hours trading, cross barrier communications…);
- Vendor has shown commitment to deliver their best technical resources to address questions and concerns;
- Multiple open-source components (e.g. elastic search) allowing for development of in-house enhancements to surveillance;
- Can be deployed to Front-Office, Compliance and Anti-Fraud teams with customized settings for each team and the ability to escalate events across groups as needed.

Answering to the research questions:

Can *Solution1* help in reducing the cost of surveillance?

As covered in the literature review Regtech offer massive cost saving opportunities in compliance (Arner, Barberis, Buckley, and Zetzsche, Dirk, 2017) and *Solution1* proves that. *Player1* is now able to adopt a supervisory structure that efficiently distributes the work across

Front-Office Supervisors and Compliance functions and resources. The capability of seeing all the relevant data within a tool without waiting for IT extractions increases monitoring and investigations.

Data collection, monitoring, analysis and reporting evolved into a completely new industry. This was fundamentally driven by advances in big data technologies (Alvarez and Marsal, 2018). *Solution1* "big data" architecture is highly scalable to cover more employees, data and use cases that legacy technology. The capability to support sophisticated analytics, house relevant data and provide real time search is fundamental to achieve efficiency.

Solution1 can therefore help in reducing the cost of surveillance. Time is saved by the intra-day surveillance capabilities and by faster targeted queries and analytics report generation. Money is saved in employee time to complete required surveillance tasks and by using one solution across the business. Regtech places compliance as a competitive advantage and not purely a cost (Wyman, 2018).

Can *Solution1* identify the employees that are putting the company at risk?

The number of false positives and the inability for a multi-vector contextual analysis is a big problem for surveillance of Electronic Communications. *Solution1* allows for the comprehension of complex interactions between employees using predictive analytics tools. Each employee has a specific layer of behavior, and layered analytics creates a more complete picture of what is happening in the organization, thus being able to identify employees that are or may put the company at risk.

Allowing for ingestion of multiple risk vectors (e.g. email, chat, trade logs, building entry logs…) to enable the holistic supervision to staff (e.g. off hours trading, cross barrier communications…). This holistic approach to supervision and regulation as covered in the literature review is one of the main breakthroughs of regulatory technology. It could eventually lead to an altogether new regulatory paradigm that will manage everything from advanced digital information to data sovereignty (Arner, Barberis and Buckley, Buckley P., 2017a).

Can *Solution1* allow for a quick response to the regulators?

This question can be split in two possible regulatory response outcomes: Adjusting to new regulatory demands and/or responding to specific regulatory queries. *Solution1* can ensure that any regulatory change is identified and incorporated into the activities. It possesses a highly configurable nature, and that is crucial to make sure the system can evolve at the same time as regulatory requirements. On the other hand, efficient and effective data analysis allows *Player1* to respond to the regulatory queries and demands faster than ever, thus ensuring deadlines are met. Regtech offers the opportunity for institutions to perform their functions more effectively and regulatory monitoring close to real time (Arner, Barberis, Buckley, and Zetzsche, Dirk, 2017).

This concludes the in-company project. The deployment of the solution is a very big step in preventing risky behavior and showing to the regulators that *Player1* is committed in adopting innovative solutions in order for supervisors to be more effective in completing their duties thus increasing trust, ensuring investor confidence and protecting the shareholders.

8 Conclusions

We studied the disruptive impact of technology in regulatory compliance within the financial sector by following the deployment of an electronic communications surveillance within a top-tier Financial Institution.

First, we documented the background that set the stage for the in-company project, by following the history of financial innovation and the impact of the 2008 Global Financial Crisis to the development of Regulatory Technology. The financial sector has forever changed and Regtech will only continue to reinvent itself. Growing post-crisis regulatory requirements and technological advances will grow in parallel creating new opportunities but also raising new risks.

Second, we presented the in-company project, starting by evaluating the risks of poor electronic surveillance mechanisms within the financial sector and the consequent need for a multi-vector surveillance tool to appropriately address the nature of these threats in a holistic manner by gathering records, discovering correlations, and providing a credible output for review, analysis, prevention and correction. Followed by going in-depth into the technicalities of the deployment of a new surveillance mechanism and framework within a top-tier Financial Institution. Banks are paying out billions of dollars in fines, penalties, and settlements for misconduct and fraud situations. In an effort to prevent this abuse, we analyzed how technology can help Financial Institutions making sure that the appropriate supervisory tools are in place to support a strong ethical and compliant culture.

Finally, while limited by confidentiality purposes, being that without those limitations this in-company project could be further developed (e.g. cost analysis, workflow presentations, examples of real cases), we were able to present the benefits of technology for conduct and surveillance purposes. Unfortunately, risky conduct and behavior will not cease to exist. Rules will eventually be broken and the cat and mouse game will last forever with new laws and new ways to circumvent them. The greed of people, institutions and governments will always pose as a peril to the entire Financial system.

Industry participants must align in order to build a safer environment for everyone, but safer doesn't mean threat free. It would be unrealistic to think that we could completely eliminate every single threat, but as this dissertation tries to show, we can surely partner with technology and do our best efforts to prevent and minimize their risks.

9 Bibliography

Alper, Alexandra and Ridley, Kirstin. "**Barclays Paying $453 million To Settle Libor Probe**"; https://www.reuters.com/article/us-barclays-libor/barclays-paying-453-million-to-settle-libor-probe-idUSBRE85Q0J720120627. June 27th, 2012.

Alvarez and Marsal. "**Regtech 2.0**". https://www.alvarezandmarsal.com/sites/default/files/regtech_2.0_report_final.pdf. February 12th, 2018.

Armstrong, Patrick. "**ESMA Regulatory Technology: Reshaping The Supervisor-Market Participant Relationship**"; Note prepared for the Europlace Financial Forum, Paris France July 12th, 2017.

Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P. "**FinTech, RegTech And The Reconceptualization of Financial Regulation**". Northwestern Journal of International Law & Business Volume 37. 2017a.

Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P. "**FinTech And RegTech In A Nutshell, And The Future In A Sandbox**". CFA Institute Research Foundation Vol. 3, Issue 4, pp. 1-20. 2017 b.

Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P. "**The Emergence Of Regtech 2.0: From Know Your Customer To Know Your Data**". Journal of Financial Transformation, vol.44, pages 79-86. 2016.

Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P. "**The Evolution Of Fintech: A New Post-Crisis Paradigm?**". University of Hong Kong working paper. 2016.

Benner, Katie. "**Baltimore The City That Sues Banks**". http://fortune.com/2012/08/30/baltimore-the-city-that-sues-the-banks/. August 30th, 2012.

Bloomberg News, "**Trader Chat Rooms Part Of Bigger Problem**". https://business.financialpost.com/investing/trader-chat-rooms-part-of-bigger-problem. November 28th, 2013.

CB Insights. "**Regtech Market Map"**.

https://www.cbinsights.com/research/regtech-regulation-compliance-market-map/. February 2017.

Chatterjee, Sumeet & Editing by Coghill, Kim. "**U.S., EU Fines On Banks' Misconduct To Top $400 Billion By 2020: Report**". https://www.reuters.com/article/us-banks-regulator-fines/u-s-eu-fines-on-banks-misconduct-to-top-400-billion-by-2020-report-idUSKCN1C210B. September 27th 2017.

CNBC. "**Volatility Index Manipulation Contributed To The Market Plunge Last Week, Whistleblower Alleges In Interview**". https://www.cnbc.com/2018/02/13/whistleblower-market-manipulation-of-vix-contributed-to-sell-off.html. February 2018.

Deloitte. "**Reputation Matters, Developing Reputational Resilience Ahead Of Your Crises**". Deloitte. https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/deloitte-uk-reputation-matters-june-2016.pdf. June 2016.

Doctors, Silver. "**Here's Just How Easy And Pervasive It Was (Is) To Manipulate The Gold & Silver Markets**". http://investingchannel.com/article/455995/Heres-Just-How-Easy-And-Pervasive-It-Was-Is-To-Manipulate-The-Gold--Silver-Markets#.W9N2TktKjIU. April 10th, 2018.

Dow Jones and SWIFT. "**2017 Global Anti-Money Laundering Survey**". http://go.dowjones.com/AMLsurvey2017. 2017.

Enriques, Luca. "**Financial Supervisors And Regtech: Four Roles And Four Challenges**". Revue Trimestrielle de Droit Financier 53. 2017.

Ferro, Shane. "**One Call From Jamie Dimon May Have Stopped The DOJ From Investigating Bankers For Fraud During The Financial Crisis**". https://www.businessinsider.com/matt-tabbi-jp-morgan-whistleblower-story-2014-11. November 6th, 2014.

FICC Markets Standard Report, "**Annual Report**". http://fmsb.com/wp-content/uploads/2017/09/FMSB_Annual_Report_Final_v2.pdf. September 2017.

FINRA. "**Regulatory Notice: Supervision Of Electronic Communications"**. https://www.finra.org/sites/default/files/NoticeDocument/p037553.pdf. December 2017.

FINRA "**Technology Based Innovations For Regulatory Compliance ("RegTech").** https://www.finra.org/sites/default/files/2018_RegTech_Report.pdf. September 2018.

FINRA "**FINRA Rule 1011".** http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=3567. 2008.

Hill, Eleanor "**Is Regtech the Answer To The Rising Costs Of Compliance?**". http://www.fx-mm.com/50368/fx-mm-magazine/past-issues/june-2016/regtech-rising-cost-compliance/. June 2016.

IIF 2016. "**Regtech In Financial Services: Technology Solutions For Compliance And Reporting**". https://www.iif.com/system/files/regtech_in_financial_services_-_solutions_for_compliance_and_reporting.pdf. March 2016.

Jones, Stephen. "**How Regtech Is Changing Banking. Proponents Of Regulation Technology Say It Can Revolutionize Compliance, And The UK Is Where Much Of The Action Is**". https://www.managementtoday.co.uk/regtech-changing-banking/future-business/article/1492799. September 14th, 2018.

J.P Morgan, Reuters, "**RiskMetrics – Technical Document**". Fourth Edition. 1996.

King, Leo. "**Bandits, Mafia, Cartel. Bank Traders' Astonishing Online Messages**". https://www.forbes.com/sites/leoking/2015/05/21/forex-barclays-citi-ubs-jpmorgan-online-chat-instant-messenger/#2f8a8aad5847. May 21st, 2015.

Klein, Aaron, "**Financial Regulation: A Post-Crisis Perspective".** Note prepared for the The Brooking Institution, Washington D.C July 14th, 2017.

KPMG, "**The Pulse Of Fintech Q2 2017**". https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/pulse-of-fintech-q2-2017.August 2017

Lin, Tom C. W. "**Compliance, Technology, And Modern Finance**". 11 Brook. J. Corp. Fin. & Com. L. 159-182. 2016.

Management Today. "**How Regtech Is Changing Banking**". https://www.managementtoday.co.uk/regtech-changing-banking/future-business/article/1492799. September 2018.

Mau, Sephanie. "**Whistle-Blower Security, Major Bank Traders Discovered To Be Trading Info In Chat Rooms**"

https://www.whistleblowersecurity.com/major-bank-traders-discovered-to-be-trading-info-in-chat-rooms/. November 14th, 2014.

Medici. "**Strategic Analysis Of Regtech: A Hundred Billion-Dollar Opportunity**". https://memberships.gomedici.com/research-categories/strategic-analysis-of-regtech-a-billion-dollar-opportunity. April 2016.

Milken Institute. "**Regtech: Opportunities For More Efficient And Effective Regulatory Supervision And Compliance**". https://assets1b.milkeninstitute.org/assets/Publication/Viewpoint/PDF/RegTech-Opportunities-White-Paper-FINAL-.pdf. July 2018.

Moody's. "**Regtech – Enabler Of The Shift from compliance to performance**". https://www.moodysanalytics.com/media/whitepaper/2018/regtech%20enabler%20of%20the%20shift%20from%20compliance%20to%20performance%20-%20survey%20results.pdf. April 2018.

Oliver Wyman. "**Regtech On The Rise: Transforming Compliance Into A Competitive Advantage"**. https://www.oliverwyman.com/content/dam/oliverwyman/v2/publications/2018/may/RegTech-on-the-Rise.pdf. 2018.

Public Banking Institute. "**Material Responsibility: What The Banks Did To Baltimore".** http://www.publicbankinginstitute.org/material_responsibility_what_the_banks_did_to_baltimore. 2012.

PricewaterhouseCoopers "**A New Dimension To The Three Lines Of Defense**". https://www.pwc.in/assets/pdfs/publications/2018/a-new-dimension-to-the-three-lines-of-defence.pdf. August 2018.

RegTechMarkets. "**RegTech Markets Directory 2017: Insights And Intelligence".** https://regtechforum.co/wp-content/uploads/2017/12/RTM-Directory-White-Paper-2017.pdf. December 2017

Smarsh, "**Electronic Communications Compliance Surveillance Report**". http://corporatecomplianceinsights.com/wp-content/uploads/2016/05/Smarsh_2016_Survey.pdf. 2016.

Tabb Group. "**Financial Markets: Embracing Regtech**".

https://hollandfintech.com/wp-content/uploads/2017/12/Tabb-Group-Report-Financial-Markets-Embracing-RegTech-April-2017.pdf. April 2017.

Transatlantic. "**The Future Of RegTech For Regulators: Adopting A Holistic Approach To A Digital Era Regulator"**. https://www.innovatefinance.com/reports/future-regtech-regulators-adopting-holistic-approach-digital-era-regulator/. June 2017.

Verschoor, Curtis, "**Did Repeal Of Glass-Steagall For Citigroup Exacerbate The Crisis?**". Strategic Finance Magazine. February 2009.

Zetzsche, Dirk Andreas and Buckley, Ross P. and Arner, Douglas W. and Barberis, Janos Nathan. "**Regulating a Revolution: From Regulatory Sandboxes To Smart Regulation**". 23 Fordham Journal of Corporate and Financial Law 31-103. 2017.