INDUSTRY IN ONE: FINANCIAL SERVICES

By

Anna Lebedeva, IGP, CIPM, PMP

Project Underwritten By:

ARMA International Educational Foundation

June 26, 2019

www.armaedfoundation.org

Table of Contents

Introduction

The purpose of this research paper is to provide a guide for records and information management (RIM) professionals transitioning into financial services from another industry or continuing their RIM career in the financial services industry. It is expected that readers have knowledge of RIM fundamentals and some experience in the field, as the basic concepts of RIM will not be covered here.

The focus of the paper is to highlight the unique aspects of managing records and information in financial services to equip readers with the knowledge and skills they need to implement a successful RIM program. The author will cover a brief history of the financial system in the U.S., financial services industry overview, various drivers behind RIM in financial services, risks affecting financial institutions and how they translate into RIM priorities, an in-depth look into specific types of records, new trends affecting RIM in the financial sector, RIM placement within organizational structure, and a future outlook on the financial industry and RIM.

Those who have spent at least a small amount of time in RIM would agree that the work is never done. The RIM program at any organization, especially in mid- to large-sized organizations, is a continuous multi-year initiative that evolves with the industry while new challenges and opportunities emerge that require constant attention and program adjustments. The scope of the RIM program at a financial services institution can seem overwhelming. The best way to approach it and make progress is to break the work into smaller, manageable pieces in order to gain “small wins” and maintain the momentum to move forward.

The complexities of managing records and information in financial services are arguably some of the toughest to solve compared to other industries primarily because of intense regulatory scrutiny. Designing a RIM program in financial services requires a pragmatic and consistent approach that supports balancing the requirements of regulatory compliance with the goals of growing the business.

1. History of the Financial System in the U.S.

In order to be ready to tackle RIM in the financial services industry it is crucial to understand the history of the financial system in the U.S. A strong and smoothly operating financial system is a significant contributor to a healthy economy and stimulates economic growth. From the establishment of the first bank in 1791, to the modern day, the financial system in the U.S. has been shaped by a cyclical trial of federal and state legislation. Over the years, the regulation reflected the conflicting forces of centralized government control to maintain stability in the financial system vs. the fear of too much control being concentrated in too few hands which resulted in deregulation.

As the banking system evolved throughout the past century, the need for increased regulation led to the creation of a nationalized banking system during the Civil War, and the creation of the Federal Reserve in 1913. After the stock market crash of 1929, with more than 10,000 banks closing their doors, the U.S. economy entered a severe economic crisis known as the Great Depression. The Depression led to even more banking regulations, such as the Glass-Steagall Act of 1933. This act separated commercial from investment banking in an effort to make financial markets more stable and minimize undue risks that depositors faced. Subsequently, the Federal Deposit Insurance Corporation was created by the Glass-Steagall Act to protect deposits. The Securities Exchange Act of 1934 created the Securities and Exchange Commission (SEC), which required that all companies offering securities to the public register and regularly file with the SEC and enabled the public to file civil charges against companies and individuals found guilty of fraud and other security violations. These new regulations were welcomed by investors who were hesitant to return to the market following World War II, the primary force that restarted the economy and ended the Great Depression.

While increased regulation resulted in a period of financial stability up until 1980, it also hurt commercial banks as they were increasing losing market share to less regulated and more innovative financial institutions, such as investment firms. For this reason, a wave of deregulation occurred throughout the last two decades of the 20th century. Congress passed several acts which served to deregulate financial institutions that accepted deposits and removed restrictions on the opening of bank branches in different states, which had been in place since 1927. However, the deregulated financial system created new complexities and led to the biggest

economic crisis since the Great Depression, the Great Recession, which started in December 2007 and ended in June 2009, despite its large size.

One of the main causes attributed to the Great Recession was the failure of the government to regulate the financial industry, specifically, irresponsible sub-prime mortgage lending. In addition, there were too many financial firms taking on too much risk. As such, investment firms grew and became competitors of commercial banks but were not subject to as much scrutiny and regulation. When some of the biggest investment firms, like Lehman Brothers, failed, it affected the availability of credit to consumers and businesses. Some economists argue that the repeal of the Glass-Steagall Act in 1999 helped cause the recession because it made it possible for some of the larger U.S. banks to merge and form bigger institutions via the creation of financial holding companies that could own both commercial and investment banks (with insurance companies as affiliates). The U.S. financial system crisis turned into a global crisis which resulted in the U.S. government having to bail out U.S. banks that became “too big to fail”, and increased its regulatory power yet again to repair the failed U.S. financial system and prevent a similar crisis from happening again.

In 2010, in response to the Great Recession, Congress passed, and President Obama signed, the Dodd-Frank Wall Street Reform and Consumer Protection Act to give the government some regulatory power over the financial system. The act established several new government agencies, such as the Consumer Financial Protection Bureau, whose purpose was to prevent predatory mortgage lending and make it easier for consumers to understand the terms of a mortgage. The Volcker Rule, a key component of the Dodd-Frank Act, restricts the ways banks can invest, specifically not allowing them to be involved with hedge funds or private equity firms, as these kinds of businesses were considered too risky. The act also introduced a new regulation for derivatives, including the requirement for them to be traded on centralized exchanges like stocks and commodities as opposed to over the counter, as that was believed to have contributed to the financial crisis.

As with any regulation, some of the provisions of Dodd-Frank were not well received by the Trump administration and some members of Congress. They felt that over-regulation introduced by Dodd-Frank was hurting the financial industry, specifically small and regional banks and small lenders; that it caused inefficiency and discouraged investments. Subsequently, in May of

2018, the House of Representatives voted to roll back significant pieces of Dodd-Frank. President Trump administration officials were also discussing the idea of reviving the Glass-Steagall Act that separated investment and consumer banking to ensure that "too big to fail" institutions do not produce an economic crisis like the Great Recession again. If history is any indication, the battle of centralized regulation vs. deregulation is not over, and the cycles will continue to repeat.

As the U.S. financial system continues to evolve in response to financial catastrophes of modern history and changing regulation, it seems apparent that some realities are here to stay: 1) financial stability of major firms is paramount to the stability of the financial system and the economy overall, and 2) financial institutions have to be more transparent and accountable when conducting business practices to protect consumers from being misled into deals that are not in the best interest of the consumers. Regulations force financial institutions to “play by the rules”. Non-compliance no longer results in just fines and bad publicity; it can put firms out of business.

Now more than ever, financial institutions are required to show evidence that their business practices are in line with regulatory requirements, and one of the best ways to do that is through sound RIM practices. Regulators and other authorities are putting extreme pressure on firms, requiring increased transparency and faster responses to data inquiries. Inadequate RIM practices have a material financial impact. Appendix 1 illustrates just a few recent records management failures highlighted in the news, and the resulting consequences.

Enhanced reporting, supervisory, and recordkeeping requirements faced by financial services firms in today’s regulatory environment are the result of the turbulent history of the U.S. financial system and require prudent and consistent implementation to withstand regulatory and legal scrutiny. Thus, the role of RIM in financial institutions has been elevated in the last two decades and requires continued focus, executive support and sponsorship, and enterprise-wide program scope to be effective at minimizing the risk of non-compliance and increasing information value.

2. Financial Services Industry Overview

Types of Financial Services Organizations

In today's financial services marketplace, a financial institution exists to provide a wide variety of deposit, lending, and investment products to individuals and businesses. While some financial institutions focus on providing services and accounts for the general public, others serve only certain consumers, businesses, or government with more specialized offerings.

To build and implement a compliant RIM program, it is important to understand the differences between the types of financial institutions to determine their specific recordkeeping obligations. The major categories of financial institutions include central banks, retail and commercial banks, internet banks, credit unions, savings and loans associations, investment banks, investment companies, brokerage firms, insurance companies, and mortgage companies. Following is a brief description of each type of financial institution.

Central Banks

A central bank is the financial institution responsible for the oversight and management of all other banks. In the U.S., the central bank is the Federal Reserve Bank, which is responsible for conducting monetary policy, and supervision of and regulation for financial institutions. Consumers do not deal directly with a central bank; instead, large financial institutions work directly with the Federal Reserve Bank to provide products and services to the general public.

Retail and Commercial Banks

Traditionally, retail banks offered products to individual consumers while commercial banks worked directly with businesses. Currently, the majority of large banks offer deposit accounts, lending, and limited financial advice to both customer segments. Retail and commercial banks offer products such as checking and savings accounts, certificates of deposit, personal and mortgage loans, credit cards, lines of credit, and business banking accounts. Most large- and medium-sized banks also have brokerage, wealth management, private banking, and insurance divisions.

Internet Banks

A newer player in the financial services marketplace is the internet bank, also referred to as a digital-only bank, which works similarly to a retail bank. Internet banks offer the same products and services as conventional banks, but they do so through online platforms instead of brick and mortar locations. Their lean and quick-to-market operational model has enabled them to gain market share, without significant investments, to meet operational and regulatory burdens that conventional banks face. (Read more on digital-only banks in Section 6 – Industry Trends and Impact on RIM.)

Credit Unions

Credit unions are not-for-profit financial organizations that are owned by and exist to serve their members, such as teachers or members of the military. Like banks, credit unions accept deposits, make loans and provide a wide array of other financial services. Any profit earned by a credit union is either invested back into the organization or paid out to members as a dividend. As a not-for-profit institution, credit unions pay no state or federal taxes and, therefore, can charge lower interest rates than banks for most financial services.

Savings and Loan Associations

Savings and loan associations are financial institutions that specialize in accepting savings, deposits, and making mortgage and other loans. Savings and loan associations provide many of the same services to customers as commercial banks, however, savings and loans associations place a stronger emphasis on residential mortgages, providing no more than 20% of total lending to businesses. Savings and loans associations are also owned and chartered differently than commercial banks, and usually serve the communities where they are located.

Investment Banks and Companies

Investment banks do not take deposits; instead, they help individuals, businesses, and governments raise capital through the issuance of securities. Investment banks specialize in large and complex financial transactions, such as underwriting, acting as an intermediary between a securities issuer and the investing public, facilitating mergers and other corporate reorganizations, and acting as a broker and/or financial advisor for institutional clients.

Investment companies pool funds from individual and institutional investors to provide them access to the broader securities market. The most commonly known example of investment companies is a mutual fund company.

Brokerage Firms

Brokerage firms act as the middleman that connects individuals and institutions that want to buy and sell securities among available investors. Customers of brokerage firms can place trades of stocks, bonds, mutual funds, exchange-traded funds, and some alternative investments. Brokerage firms typically get paid by receiving a commission (either a flat fee or a percentage of assets under management). There are several different types of brokerage firms offering a wide range of products and services, ranging from more expensive full-service brokers, to discount brokers, to low or zero cost roboadvisers.

Insurance Companies

Insurance companies are a type of “non-bank” financial institution that help individuals transfer risk of loss. Individuals and businesses use insurance companies to protect against financial loss due to death, disability, accidents, property damage, and other losses.

Mortgage Companies

Financial institutions that originate or fund mortgage loans are mortgage companies. While most mortgage companies serve the individual consumer market, some specialize in lending options for commercial real estate only.

This paper does not address recordkeeping obligations for all types of financial institutions listed above, but rather focus on retail and commercial banks, investment banks and companies, and brokerage firms, as they collectively comprise the largest number of U.S. financial institutions, and address the majority of recordkeeping requirements, including the most stringent ones to comply with.

Major Regulators, Self-Regulatory Organizations, and Industry Associations

Federal and state governments have many agencies that regulate and oversee financial institutions. While these agencies each have specific responsibilities, they work to accomplish similar goals - to regulate the financial industry and protect those who utilize the services. Their areas of coverage often overlap, but while their policies may vary, federal agencies usually supersede state agencies. However, this does not mean that state agencies have less power, as their responsibilities and authorities are far-reaching. Following are some of the major financial services regulators, self-regulatory organizations, and industry associations.

Federal Regulators

Federal Reserve Board

The Federal Reserve Board (FRB) is one of the most recognized of all the regulatory bodies. The FRB is responsible for regulating and supervising the U.S. banking system, which is intended to provide overall economic financial stability in the U.S. It influences money, liquidity and overall credit conditions. It implements monetary policy via its open market operations, which control the purchase and sale of U.S. Treasury securities and federal agency securities. Such purchases and sales determine the federal funds rates and modify the level of reserves available.

Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation (FDIC) was created by the Glass-Steagall Act of 1933 to provide insurance on checking and savings deposits at banks. The current limit is $250,000 per depositor at any of its member banks. As of 2018, the FDIC insured deposits at over 5,600 institutions[1]. This agency is also responsible for analyzing and supervising the safety and stability of financial institutions by performing consumer protection functions and managing failed banks. The trigger for creating the FDIC was the run on banks during the Great Depression when a large number of customers withdrew their money simultaneously because of concerns about the soundness of the banks.

Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency (OCC) is one of the oldest federal agencies and was established in 1863 by the National Currency Act. Its main purpose is to supervise, regulate, and provide charters to banks operating in the U.S. to ensure the soundness of the overall banking system. This supervision enables banks to compete and provide efficient banking and financial services. The OCC oversees several areas including capital, asset quality, management, earnings, liquidity, sensitivity to market risk, information technology, compliance, and community reinvestment.

Office of Thrift Supervision

The Office of Thrift Supervision (OTS) was established in 1989 by the Department of the Treasury. It is funded solely by the institutions it regulates. The OTS is similar to the OCC except that it regulates federal savings associations, also known as thrifts, or savings and loans.

Securities and Exchange Commission

The SEC was established in 1934 by the Securities Exchange Act and is among the most powerful and comprehensive financial regulatory agencies. The SEC enforces federal securities laws and regulates a large portion of the securities industry, including the U.S. stock exchanges, options markets, and options exchanges, as well as all other electronic securities exchanges and markets. It also regulates investment advisors, investment companies, and broker-dealers. The purposes of the agency are to protect investors against fraudulent and manipulative practices, promote full public disclosure, and watch over corporate takeovers in the U.S.

Commodity Futures Trading Commission

The Commodity Futures Trading Commission (CFTC) was created in 1974 as an independent authority to regulate commodity futures and options markets. This agency protects traders from market manipulation, investigates abusive trading practices and fraud, and maintains fluid processes for clearing. The CFTC oversees a variety of individuals and organizations, including swap execution facilities, derivatives clearing organizations, designated contract markets, swap dealers, major swap participants, futures commission merchants (FCM), commodity pool operators, and other entities. Starting in 2000, the agency joined forces with the SEC to help regulate single stock futures.

The Consumer Financial Protection Bureau

The Consumer Financial Protection Bureau (CFPB) is a regulatory agency that oversees all finance-related products and services provided to consumers. This agency is divided into several different units, including the Office of Fair Lending, consumer complaints, research, community affairs and the Office of Financial Opportunity. The CFPB's goal is to educate consumers about financial products and services that are available to them, and to provide another level of consumer protection through its oversight of financial services.

State Regulators

State Bank Regulators

State bank regulators operate similarly to the OCC, but at the state level for state-chartered banks. Their oversight works in conjunction with the Federal Reserve and the FDIC.

State Securities Regulators

These agencies augment the Financial Industry Regulatory Authority (FINRA) and the SEC for matters associated with regulation in the states' securities business. They provide registrations for investment advisors who are not required to register with the SEC and enforce legal actions with those advisors.

Self-Regulatory Organizations

Financial Industry Regulatory Authority

FINRA was created in 2007 from its predecessor, the National Association of Securities Dealers (NASD). FINRA is an independent nonprofit organization that acts as a self-regulatory organization. While the SEC is the ultimate regulatory authority for the industry, FINRA plays an important role when it comes to protecting investors. FINRA oversees all brokerage firms that are in the securities business with the public. FINRA's mission is to ensure "that every investor receives the basic protections they deserve, anyone who sells a securities product is licensed and qualified, securities advertisements are not misleading, all securities sold to investors are suitable for their individual needs, and investors receive a complete disclosure before purchasing any investment products". [2] It is also responsible for overseeing the mediation and arbitration processes for disputes between customers and brokers.

National Futures Association

The National Futures Association (NFA) was created in 1982 as a self-regulatory body when Congress passed an amendment to the Commodity Exchange Act. NFA assists the CFTC in its oversight functions. The original purpose of the NFA was to register introducing brokers, commodity pool operators and commodity trading advisors. In addition, the organization aims to safeguard the integrity of newer financial instruments, such as the derivatives market. As the overseer of the commodities and futures industry in the U.S., the NFA helps protect investors from fraudulent futures activities and resolve consumer complaints. The main goal of the NFA is to uphold investor confidence to safeguard a successful futures market.

Industry Associations

Securities Industry and Financial Markets Association

The Securities Industry in Financial Markets Association (SIFMA) is the leading trade association representing broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. “The combined businesses of SIFMA’s members represent 75% of the U.S. broker-dealer sector by revenue and 50% of the asset management sector by assets under management” (SIFMA.org, 2019).[3] SIFMA is the U.S. regional member of the Global Financial Markets Association (GFMA). SIFMA advocates for effective and resilient capital markets and provides a forum for industry policy and professional development.

International Swaps and Derivatives Association

The International Swaps and Derivatives Association (ISDA), established in 1985, is a leading trade association with over 900-member institutions from 69 countries, and its goal is to make the global derivatives markets safer and more efficient. ISDA membership is comprised of a broad range of derivatives market participants including corporations, investment managers, government and supranational entities, insurance companies, energy and commodities firms, and international and regional banks.

Futures Industry Association

The Futures Industry Association (FIA) is a leading global trade organization for the futures, options, and over-the-counter cleared derivatives markets. Its mission is to support open, transparent, and competitive markets, protect and enhance the integrity of the financial system,

and promote high standards of professional conduct. FIA’s members include firms registered with CFTC as FCM. Many of these FCMs are also registered as broker-dealers with the SEC.

3. Drivers for RIM in Financial Services

Main Regulations that Drive RIM Requirements

As noted earlier, there have been many financial regulations throughout the history of the financial system in the U.S. The main goals of regulations are to ensure consumer protections, ethical and sound business practices, and the stability of the financial system overall. Many of the financial services regulations include requirements for sound recordkeeping as a way to demonstrate the transparent and accountable business practices. Following are the significant recordkeeping regulations grouped by the financial entity type (registration).

Broker Dealers

By far, the most stringent recordkeeping regulations in the U.S. are imposed by the Securities and Exchange Act (SEA) of 1934 on the securities broker-dealer industry. The following are the key recordkeeping rules:

17 CFR § 240.17a-3

SEA Rule 17a-3 applies to certain national securities exchange members and broker-dealers, and defines the types of books and records related to the business of broker-dealer as such to be made and kept current.

17 CFR § 240.17a-4

SEA Rule 17a-4 compliments the SEA Rule 17a-3. 17a-4 defines additional categories of books and records to be preserved by certain national securities exchange members and broker-dealers, and specifies the retention requirements for books and records defined in 17a-3 and 17a-4. In 1997, the SEC revised rule 17a-4(f) by expressly allowing books and records to be retained on electronic storage media, subject to explicit conditions. Additionally, FINRA Rule 4511 explicitly defers to the format and media requirements of SEA rule 17a-4 for the books and records it covers. The current recordkeeping requirements of rule 17a-4 include:

1) A minimum stated retention period based on the type of books and records (3 or 6 years),

2) A notification that books and records are to be stored for 2 years in an easily accessible place,
3) The description of the electronic storage form, such as micrographic media (microfilm, microfiche) or electronic storage media (electronic storage system) that meets requirements of 17a-4(f)(2),
4) A notification to the designated examining authority (FINRA) at least 90 days prior to utilizing any electronic storage media,
5) Preservation of books and records in “non-rewritable, non-erasable” or “write once, read many” (WORM) format,
6) Serialization (date and time of recording in combination with unique identifier) of original and duplicate units of storage media,
7) The ability to readily download indexes and records preserved on electronic storage media to any medium acceptable under the rule required by SEC or FINRA,
8) A duplicate copy of the record stored separately from the original and on medium that meets the requirements of 17a-4(f),
9) A duplicate copy of the index stored separately from the original and on medium that meets the requirements of 17a-4(f),
10) Preservation of the original and duplicate copies of the index for the same time as the records they relate to,
11) An audit system (audit trail) to capture the input of records onto electronic storage media and any changes made to the original and copies of the records, the ability to have the audit system available for examination by the SEC or FINRA, and the preservation of the audit system results for the same time as the audited records
12) Designated Third Party (D3P) consultant access to the records with the ability to download information on electronic storage media and file written undertaking with FINRA, and
13) Third parties who preserve records on behalf of the member, broker or dealer to file written undertaking with SEC that they will preserve the records in a manner compliant with the requirements of 17a-4(f), allow examination of books and records by the SEC, and produce the records if requested.

While not specifically defined, SEC staff indicates that the storage of records outside of the U.S. is not permitted. Broker-dealers are the only U.S.-registered financial institutions that are still required to comply with WORM storage requirements. Since those requirements are the strictest in the industry, compliance with the SEC 17a-4 recordkeeping rule will warrant compliance with all other recordkeeping rules that may be applicable to firms in the U.S.

Challenges of WORM Standard

WORM systems are costly, outdated, and inefficient storage systems used exclusively to meet the requirements of Rule 17a-4. Data stored on WORM is essentially a static snapshot in time of a record and cannot be used to stand up a production system during or following a disaster event. WORM technology is not suited to fulfill backup and recovery needs of dynamic financial institutions that are performing millions of transactions in real-time communications with customers. It results in firms having to maintain multiple backup and failover systems in addition to the SEC-required WORM systems.

Additionally, WORM systems are not programmed to work with customer-facing communications systems that provide records to customers such as websites, voice response units, and emerging communication tools. WORM systems are not flexible enough to store dynamic content generated by complex trading and risk systems, as well as records created by aggregating information from various systems. The complexity of source information makes effective WORM storage costly and difficult. Complex databases that store general ledgers, trading data, blotters, and other data collate it into a structured record that may change several times every second, and any attempt to retain such a structured record in WORM format only reflects a “point-in-time picture.” During examinations regulators will request data to be produced from online production systems before it has been transferred to WORM because it can be readily sortable and searchable.

The firms are required to invest significant capital into WORM storage systems that serve a very narrow purpose. This requirement becomes particularly burdensome to meet for broker-dealers engaged in multiple businesses, such as selling commodities, futures, swaps, and mutual funds that are subject to multiple regulators (SEC, CFTC, OCC, FRB, etc.). Many trading systems comingle different types of records, so it becomes extremely costly for firms that cannot

segregate records by regulations. It forces them to retain non-broker-dealer records in the high-cost WORM format when they are not legally required to do so. The cost of WORM technology may also push smaller firms out of the market, as only larger firms may be able to afford to acquire and maintain such costly recordkeeping systems.

According to SIFMA, its members estimate that a cost to implement a WORM storage system at a large firm is on average $10 million dollars. Several SIFMA members reported that the implementation took more than 3 years with 10-45 employees spending at least 50% of their time on the effort during that period. WORM compliance recordkeeping costs are not limited to implementation. SIFMA member firms spend an additional $1.2 million dollars annually for maintenance. These estimates do not include costs related to implementing WORM storage for each business application producing SEC-regulated records, or costs related to the D3P service.[4] SIFMA and its members express that the costs of complying with rule 174-4(f) outweigh any perceived benefit of this outdated rule.

For the reasons described above, on November 14, 2017, SIFMA, in cooperation with other industry associations, filed a petition with SEC on behalf of its broker-dealer members to amend SEA Rule 17a-4(f) and remove WORM, 90-day notification of intention to use electronic storage media, D3P, and audit system requirements. As of the writing of this paper the SEC has not amended the recordkeeping rule.

FINRA Rule 4511

FINRA Rule 4511 requires its members to preserve books and records as required under the FINRA rules as well as SEA rules. It is a “catch-all” rule that states that those FINRA books and records, for which there is no specified period under the FINRA rules or applicable SEA rules, are to be retained for a period of at least 6 years in a format and media that comply with SEA Rule 17a-4(f).

FINRA Rule 3110

As it relates to recordkeeping, FINRA Rule 3110 mandates that each member firm creates and maintains written supervisory procedures which set forth, discuss, and explain the

testing, review, and supervision of the firm's compliance with WORM record retention requirements as defined in SEA Rule 17a-4(f).

FINRA Rule 2210

FINRA Rule 2210, commonly referred to as Advertising Rule, covers recordkeeping requirements for communications with the public that can fall into one of the 3 communication categories:

1) Correspondence - any written communication distributed or made available to 25 or fewer retail investors within any 30 calendar-day period.
2) Retail communications - any written communication distributed or made available to more than 25 retail investors within any 30 calendar-day period. Communications that formerly qualified as "advertisements" and "sales literature" in an older version of the rules generally now fall under the definition of retail communications.
3) Institutional communications - any written communication distributed or made available only to institutional investors but does not include a member's internal communications.

Firms must maintain all correspondence in accordance with the recordkeeping requirements of SEA Rule 17a-4(f) and FINRA 4511.

All retail and institutional communications must be retained for the retention period required by SEA Rule 17a-4(b) and in a format and media that comply with SEA Rule 17a-4(f). The records must include:

- A copy of the communication and the dates,
- The name of the registered principal who approved the communication and the date of approval, and
- Information concerning the source of any statistical table, chart, graph or other illustration used in the communication.

Modern forms of electronic communications, such as publicly available websites, password-protected websites, banner advertisements, bulletin boards, social media, and instant messaging, are examples of retail communications that are covered under FINRA Rule 2210. A registered principal of the firm must approve all static content (content generally accessible to all visitors

that remains posted until it is removed by the firm) before it is posted. Interactive content (real-time communications) does not require approval by a registered principal prior to use. FINRA Rule 2210 specifically exempts from pre-review any retail communication that:

- Is posted on an online interactive electronic forum, and
- Does not make any financial or investment recommendation(s) or otherwise promote a product or service of the firm.

However, firms still have recordkeeping requirements and must supervise communications. Refer to Section 5 – Electronic Communications – Retention and Supervision for more information on recordkeeping requirements for electronic communications.

Investment Companies, Financial Advisers

In 2001 the SEC specifically considered and rejected WORM storage requirements for investment companies and investment advisers, choosing instead principles-based electronic storage requirements for these entities.[5] The SEC did not actually demonstrate that they found more issues with broker-dealers than investment advisers, but only stated that they had not experienced any significant issues with records being altered by financial advisers.

Investment Advisers Act Rule 204

The Investment Advisers Act of 1940, also called the "Advisers Act", Rule 204-2 applies to registered investment advisers and defines the types of books and records relating to their investment advisory business to be made and kept true, accurate, and current. Recordkeeping requirements of Rule 204 state that:

1) Generally, most books and records must be kept for 5 years from the last day of the fiscal year in which the last entry was made on the document or the document was disseminated; however, certain records must be kept for longer periods.
2) Records are to be kept in an easily accessible location, such as the firm's principal office. Many advisers store duplicate copies of their advisory records in a location separate from their principal office in order to ensure the continuity of their business in the case of a disaster.

3) Records can be stored using either micrographic media or electronic media, including microfilm and magnetic disk, tape, or other computer recordkeeping devices. If using email or instant messaging to make and keep the records that are required under the rule, all attachments need to be included as part of the complete record.
4) Electronic records are to be protected from unauthorized access and theft, or unintended destruction.
5) Records are to be indexed to allow easy location, access, and retrieval of any particular record.
6) Ability to promptly (generally within 24 hours) produce required electronic records that may be requested by the SEC, including email.

Swap Dealers, Major Swap Participants, and Futures Commission Merchants

The key recordkeeping rule under CFTC is 17 CFR § 1.31. To be consistent with similar requirements that the SEC had implemented in 1997, in 1999 the CFTC implemented WORM and other requirements when it permitted books and records to be stored electronically. The requirements of CFTC rule 1.31(b)-(c) were very similar in principal and context to requirements stated in SEA Rule 17a-4. On May 30, 2017, after careful consideration and industry dialogue, the CFTC amended its recordkeeping rule 1.31, which modernized recordkeeping obligations for CFTC regulated records. The new rules afford regulated entities "greater flexibility regarding the retention and production of all regulatory records under a less-prescriptive, principles-based approach."[6] Key changes of rule 1.31 include the elimination of native file format, WORM, third-party consultant, chain of custody (audit system), written policies and procedures requirements, and a new retention period for pre-trade swaps and forwards communications.

17 CFR § 23.201

17 CFR § 23.201 defines the types of swap dealer and major swap participants' records regulated by the CFTC, including transaction and position records, financial and marketing records, complaints, and records of data reported to a swap data repository.

17 CFR § 23.202

17 CFR § 23.201 defines the types of swap dealer and major swap participants' records regulated by the CFTC, including daily transaction records for swaps (pre- and post-execution), and daily trading records for related cash and forward transactions.

17 CFR § 1.31

The current recordkeeping requirements of rule 1.31 state:

1) A replacement of the term "books and records" with "regulatory records", which includes complete records together with all pertinent data and memoranda of all activities related to the business of the regulated entity.
2) A minimum retention period for regulatory records based on the record type and format (mainly 5 years, and 1 year for oral communications).
3) Regulatory records are to be readily accessible via real-time electronic access for first 2 years of the retention period, and retrievable from storage within 3 business days during the remainder of the retention period.
4) Form and manner to ensure the authenticity and reliability of the regulatory records,
5) For electronic regulatory records:
    a. Systems that maintain the security, signature, and data as necessary to ensure authenticity of the information,
    b. Systems that ensure the records can be produced and are available in the event of emergency or other disruption of electronic record retention systems, and
    c. The creation and maintenance of an up-to-date inventory of systems that store regulatory records.
6) Regulatory records must be open to inspection by the CFTC, U.S. Department of Justice, or any applicable prudential regulator,
7) The production of regulatory records is to be made promptly upon request and in the medium requested.

17 CFR § 23.203

17 CFR § 23.203 prescribes requirements for the location of records to be retained. All records required to be kept by a swap dealer or major swap participant must be kept at the principal place of business. If the principal place of business is outside of the US, then the swap dealer or major swap participant must provide the records as requested at the place in the U.S. designated by the representative within 72 hours after receiving the request. The storage and management of swap dealer, major swap participant, and FCM records by third-parties is not explicitly permitted.

In addition, each swap dealer and major swap participant must maintain for each of its offices a listing of each person at that office who, without delay, can explain the types of records the swap dealer or major swap participant maintains at that office and the information contained in those records.

Retail and Commercial Banks

There are numerous regulations from various banking regulators mandating retention requirements for retail and commercial banks, too many to mention in this paper. However, there are a few key regulations worth noting.

12 CFR § 202.12

12 CFR § 202, also known as Regulation B, issued by the Board of Governors of the Federal Reserve System, pursuant to the Equal Credit Opportunity Act of the Consumer Credit Protection Act, defines information collection requirements and applies to all financial institutions who extend credit. The purpose of this regulation is to promote the availability of credit to all creditworthy applicants and prohibit creditor practices that discriminate on the basis of race, color, religion, national origin, sex, marital status, or age.

12 CFR § 202.12 outlines that the lending institution must retain applications of credit for 25 months (12 months for business credit) after the date that it notifies an applicant of action taken on an application or of incompleteness. The lending institution must retain in original form or a copy the following information:

1) The application and any other written or recorded information used in evaluating the application and not returned to the applicant at the applicant's request,
2) The notification of action taken,
3) The statement of specific reasons for adverse action, and
4) Any written statement submitted by the applicant alleging a violation of the Act or the regulation.

12 CFR § 226.25

12 CFR § 226, also known as Regulation Z, is issued by the Board of Governors of the Federal Reserve System to implement the Truth in Lending Act. The purpose of this regulation is to promote the informed use of consumer credit by requiring disclosures about its terms and cost. The regulation also gives consumers the right to cancel certain credit transactions that involve a lien on a consumer's principal dwelling, regulates certain credit card practices, and provides a means for fair and timely resolution of credit billing disputes.

12 CFR § 226.25 requires the lending institution to retain records that evidence compliance with the regulation for 2 years after the date disclosures are required to be made or action is required to be taken. In addition, the lending institution must make the relevant records available for inspection by the regulator.

12 CFR § 228.43

12 CFR § 228, also known as Regulation BB, is issued by the Board of Governors of the Federal Reserve System to implement the Community Reinvestment Act (CRA). In enacting the CRA, Congress required each appropriate federal financial supervisory agency to assess an institution's record of helping meet the credit needs of the local communities in which the institution is chartered.

Part 12 CFR § 228.43 mandates that banks retain:

1) A public file that includes the following:
    a. All written comments received from the public for the current year and each of the prior 2 calendar years that specifically relate to the bank's performance in

helping to meet community credit needs, and any response to the comments by the bank,

b. A copy of the public section of the bank's most recent CRA Performance Evaluation prepared by the Board,
c. A list of the bank's branches, their street addresses, and geographies,
d. A list of branches opened or closed by the bank during the current year and each of the prior 2 calendar years, their street addresses, and geographies,
e. A list of services generally offered at the bank's branches and descriptions of material differences in the availability or cost of services at particular branches, if any,
f. A map of each assessment area showing the boundaries of the area and identifying the geographies contained within the area, either on the map or in a separate list, and
g. Any other information the bank chooses.

2) Additional information available to the public such as Home Mortgage Disclosure Act (HMDA) data, the bank's loan-to-deposit ratio for each quarter of the prior calendar, etc.
3) The location of public information for inspection upon request.

Multiple Registrations

31 CFR § 103

31 CFR § 103, issued by the Monetary Offices of the Department of the Treasury, outlines the requirements for financial recordkeeping and reporting of currency and foreign transactions and applies to virtually all types of financial institutions. Some examples of records covered under this regulation include: Currency Transaction Reports, Suspicious Activity Reports, Bank Secrecy Act records, Office of Foreign Asset Control records, reports of transactions with foreign financial agencies, payment orders, foreign exchange transaction records, and records of transfer of currency or other monetary instruments, funds, checks, investment securities, or credit, of more than $10,000 to or from any person, account, or place in the U.S.

The financial institutions must retain the original or a microfilm, other copy, or electronic record pursuant to the regulation. Records required to be kept must be retained by the financial institution for a period of 5 years and must be made available to the regulator upon request at any time.

17 CFR § 248

17 CFR § 248, also known as the Volcker Rule, issued by the Board of Governors of the Federal Reserve System under section 13 of the Bank Holding Company Act, establishes prohibitions and restrictions on proprietary trading and on investments in, or relationships with, covered funds by certain banking entities, including state member banks, bank holding companies, savings and loan holding companies, foreign banking organizations, and certain subsidiaries thereof. Each banking entity must develop and maintain a compliance program reasonably designed to ensure and monitor compliance with the regulation. The terms, scope and detail of the compliance program must be appropriate for the types, size, scope and complexity of activities and the business structure of the banking entity.

17 CFR § 248.20 requires banking entities to retain records that demonstrate compliance and effectiveness of the compliance program, for a period of no less than 5 years, in a form that allows it to promptly produce such records to the regulator on request.

15 UCS 7201

15 UCS 7201, also known as the Sarbanes-Oxley Act or SOX, was developed to protect shareholders and the general public from accounting errors and fraudulent practices in enterprises, and to improve the accuracy of financial reporting. Section 802 of SOX focuses on business data retention and protection, and contains 3 rules that affect recordkeeping:

1) Destruction, falsification, and/or alteration - This rule relates to the intended alteration, destruction, falsification, or concealment of business records or documents with the intent to obstruct, impede or influence a legal investigation.
2) Retention period - This relates to the length of time business records should be retained. The length of time varies by business record type. Some examples are receivable or

payable ledgers and tax returns (7 years), employment applications (3 years), and invoices to customers (5 years).

3) Data types - This rule outlines a high-level classification of business records that must be retained and stored and includes records like electronic communications (emails), business records (i.e. invoices, bills, checks, bank statement), and general communications (i.e. letters, memos, publications).

Section 802 defines mostly the type of business records to be stored and for how long, but not how an enterprise should store its records, other than it is the IT department's responsibility to store electronic records.

Other Regulations Affecting RIM

In addition to U.S. financial services regulators mandating recordkeeping obligations on its member firms, there are other regulations in the U.S. and globally that impact the records management practices of U.S. financial institutions. Generally, those regulations cover data privacy and information security, and include limitations on data retention and requirements for data disposition.

The U.S. has a sectoral approach to privacy protection as different economic sectors, such as financial services and healthcare, operate under different legal requirements. In contrast to European laws that define privacy as a fundamental human right, the U.S. Constitution does not explicitly provide a right to privacy. A few examples of U.S. federal privacy laws are the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), and Freedom of Information Act (FOIA). Some federal privacy laws, such as FCRA, preempt state law so that states cannot make additional requirements. Others do not preempt state law, and stricter privacy protections can be added at the state level. Following are few key privacy and information security regulations impacting RIM in the U.S.

General Data Protection Regulation

General Data Protection Regulation (GDPR) is a general set of rules to protect the data privacy and security of European Union (EU) residents, but its impact is global. It went into effect in May of 2018. Although it is an EU regulation, financial institutions in the U.S. are

impacted if they manage and process data about EU residents. Since GDPR is already in effect, most global financial institutions would have already had to establish GDPR compliance programs to prepare themselves for the regulation.

GDPR sets forth the requirement for the records of data processing activities to be kept by data controllers, processors, and their representatives and make them available to supervisory authorities upon request. The types of information to be kept includes, but is not limited to: 1) the name and contact information of the controller, the representative, where applicable, and the data protection officer; 2) the purposes of the processing; 3) a description of the categories of data subjects and categories of personal data; 4) the categories of recipients to whom the data is or will be disclosed, including those in third countries; 5) information on transfers to third countries of international organizations and documentation of safeguards for the transfer; and 6) retention or erasure time limits for categories of data. GDPR allows the data subject to request a copy of their personal information retained by the firm, and those data requests must be responded to within 30 days of the request.

GDPR's data retention requirement mandates that the personal information of EU residents be kept only for as long as necessary to fulfill the original basis for collecting and processing it. The few exceptions that would permit a prolonged retention are if the data needs to be retained for regulatory/legal reasons, such as a specified regulatory retention requirement or legal investigation, for archiving purposes in the public interest, for scientific or historical research, for statistical purposes, or if the data is anonymized and thus no longer allows identification of a data subject. Following through on the retention requirement under GDPR and deleting personal data is one of the most difficult tasks an organization may attempt to do.

Another key component of GDPR that has impact on RIM is the right of EU data subjects to request deletion of their personal information. Data destruction efforts might compromise systems as data is intertwined between systems and deleting key elements of personal data in one system may lead to other data, or the whole system, losing data integrity, making it unusable or corrupted. Many legacy systems are not designed to allow for deletion of data, thereby requiring that fields be overwritten with anonymizing text rather than deleting altogether. This is extremely time consuming and, for many organizations, will require additional resources to complete data erasure by the deadline mandated by the regulation.

California Consumer Privacy Act

California Consumer Protection Act (CCPA) is the first comprehensive "GDPR-like" privacy law in the U.S. It is going into effect in January of 2020, but has a one-year lookback rule, which means that CCPA readiness must include the ability to fulfill data requests going back 12 months from the date of the request. With a population of close to 40 million people, California (CA) is one of the largest economies in the world, and ramifications of CCPA for financial institutions across the U.S. and beyond are significant. CA was the first state in the U.S. to pass data breach notification law in 2005, and now all 50 states have data breach notification laws, though details vary. CA is again a leader and the first state to pass state privacy law, with follow-on privacy legislation being drafted in 11 other states at the time of this publication. If and when the federal privacy regulation comes into existence, it is expected that CCPA will set the minimum standard for that regulation.

The definition of personal information under CCPA is broader than under GDPR and includes information that relates to, or is capable of being associated with an individual, device, or household. According to one large retailer, the broader definition of personal data led to a 300% increase in a number of systems with in-scope data at that company. Firms cannot assume that they are automatically ready for CCPA because they implemented GDPR compliance programs. They have to modify their GDPR practices to be compliant with CCPA.

CCPA applies to for-profit entities that both collect and process personal information of CA residents and do business in CA together with other criteria. CCPA may apply to consumers who are in CA for indefinite periods, and to CA residents who are outside of the state for a brief time. The purpose of the regulation is to provide consumers with more rights with respect to their personal information. Under CCPA, consumers have a right to request a copy of their personal information retained by the firm and those data requests must be responded to within 45 days of the request.

Like GDPR, one of the key consumer rights granted by CCPA that has impact on RIM is the right to request a business to delete any personal information about the consumer collected by the business (with certain exceptions).

Unlike GDPR, another key right provided by CCPA is that consumers can also direct the business to not sell their personal information to third parties (referred to as "right to opt-out"). "Sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by a business to another business or third party for monetary or valuable consideration (with some exceptions.)

GLBA-regulated financial institutions that collect, process, sell, or disclose personal information are exempt from a number of requirements under CCPA, however, it should not be interpreted as a full exemption. GLBA-regulated entities will remain subject to the provisions and requirements of the CCPA if they engage in activities falling outside of the GLBA—which they almost certainly do.

New York State Department of Financial Service 23 NYCCR 500 – Cybersecurity Requirements for Financial Services Companies

The New York State Department of Financial Service (NYDFS) 23 NYCCR 500 is a cybersecurity regulation affecting financial services organizations doing business in the State of New York. It went into effect in March of 2017 and set forth the minimum standards for cybersecurity programs. The purpose of NYDFS 23 NYCCR 500 is to protect customer information and the information technology systems of regulated entities. It requires firms to assess their information security risk profiles and design a cybersecurity program that addresses the risk in a robust fashion. The key sections of the regulation that have impact on RIM are:

1) 500.06 – Regulated entities must keep records that can be used to reconstruct material financial transactions for not fewer than 5 years, and audit trail records designed to detect and respond to cybersecurity events for not fewer than 3 years;
2) 500.13 – Regulated entities must, on a periodic basis, dispose of any non-public information that is no longer necessary for legal and business purposes;
3) 500.17 – Regulated entities must retain all records, schedules, and data supporting the annual attestation for the period of 5 years, and such documentation must be available for inspection by the regulator.

Combining Data Privacy, Cybersecurity, and RIM

As illustrated by the above examples of privacy and cybersecurity regulations impacting RIM, it is important for organizations today to rethink how they look at data and records and develop a combined approach for broader information management that involves collaborative efforts of Business, Legal, Data Governance, Privacy, Information Security, and RIM professionals to build a coordinated, comprehensive, and agile information management program to include records, non-records, and data. To make it manageable, it is best to divide the program into 3 phases:

Data mapping is the first and most critical step in building an information management program because it documents attributes related to data and information that an organization owns. Data mapping is a large effort as it takes into account business processes, data flows, applications, sensitive data inventory, records, and retention schedules. This process will help identify where the personal data is created, received, used, stored, shared, and disposed or archived. One of the approaches for data mapping that was successfully utilized by clients of BDO, one of the leading industry consulting firms, is presented in Figure 1.[7]

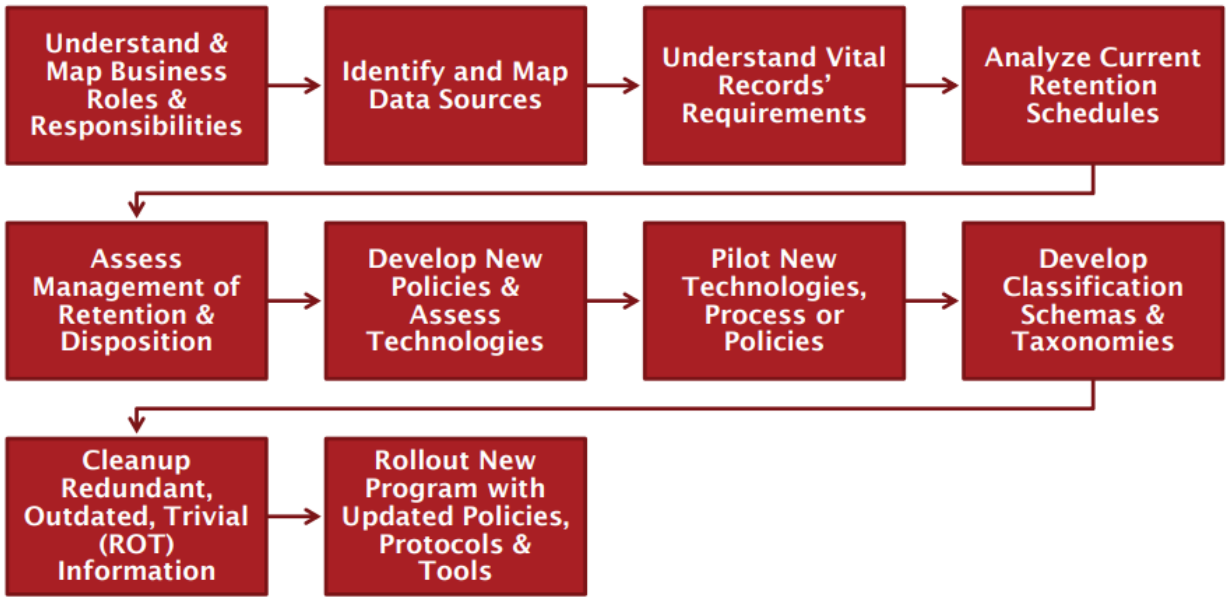

Figure 1 – Data Mapping Process **Source: BDO, September 20, 2017**

The data mapping exercise can be performed using interviews, existing technology, such as scanning, software asset management, or data loss prevention tools that can be repurposed for data mapping, or new specialized tools, or a combination of several approaches.

It is important to assess existing policies for acceptable use, information security classification, records management, legal hold management, enterprise risk, business continuity, IT operations, and internal audit to align them with data privacy and information security requirements and to develop new policies, if necessary.

Data mapping leads to the identification of gaps that will need to be prioritized based on risk. The organization will then have to develop remediation plans for each gap with a target roadmap for implementation. Instead of waiting for a data breach to raise the importance of sound information management and protection of personal information, it is recommended that organizations take a proactive approach and institute defensible disposition processes starting with records in records management repositories, followed by non-records in file shares and SharePoint, and, finally, unstructured and structured data in operational systems and databases. (Read more on approaches for cleaning up data in Section 4 - Risk Management and RIM.) Proactively cleaning up the data not only helps protect the personal information of both

customers and employees, it also allows ongoing visibility into the organization's data repositories and enables building a sustainable long-term information governance strategy that, at its best, increases the value of business information.

Other Drivers for RIM

While intense regulatory pressure is the main driver for RIM in the financial services industry, it is not the only driver. Following are several other drivers that can help make the business case for RIM.

Business Needs

Similarly to other industries, recordkeeping requirements also stem from the business need to retain information to maintain operational activities and provide products and services to customers.

Business Continuity

Disasters such as the 9/11 terrorist attack, Hurricane Katrina, and Superstorm Sandy served as an awakening for many organizations. These events made firms realize that disasters really happen, and their firm could be the next one to be affected. Disaster recovery and business continuity must be carefully planned as firms that are not well prepared can possibly be affected so severely that they go out of business. The focus must be on the vital records that are necessary to resume operations in the event of a disaster, and managing those records is part of an overall RIM program.

Maintaining Corporate Legacy

The firms also need to keep records of historical nature to maintain the corporate legacy. Such historical and vital records (those without which the firm cannot operate or restart operation) are typically retained permanently as part of organization's documentary heritage. Long-Term Digital Preservation is a key area in which RIM policy should be applied. The frailty of electronic storage media, combined with ongoing and sometimes rapid changes in computer software and hardware, poses a big challenge to ensuring access to readable and usable electronic content over time. Every electronic repository storing historical or vital records must have a strategy to mitigate computer technology obsolescence.

Litigation Risk

In 2006 the U.S. Federal Rules of Civil Procedure (FRCP) were amended to include specific requirements for legal discovery of electronically stored information (ESI) during civil litigation. The changes had a major impact on how the firms had to handle electronically generated evidence requiring them to implement formal RIM and e-discovery programs to meet the new requirements. The U.S. is one of the most litigious countries in the world which creates the need to properly manage records and information during litigation.

The firms must be able to produce requested ESI reasonably quickly, and if they fail to do so, or fail to do so within the prescribed timeframe, it can result in sanctions. This requirement dictates that firms put in place legal hold management, RIM, and defensible disposition policies and procedures. Legal hold notification management is the absolute minimum the firms should implement to meet the court rules. Legal teams work very closely with RIM professionals to identify the sources of relevant ESI since RIM experts typically have the most organizational knowledge of various information repositories containing records and non-records, as documented in data maps. RIM Professionals are also instrumental in helping Legal teams with identifying relevant paper records because they usually have direct access to the paper inventory, whether onsite or at an offsite vendors' storage location.

Perhaps the most important benefit of having sound RIM and e-discovery programs is that they lay foundation for the firms to move to defensible disposition, the process that not only helps with the cleanup of information that no longer has business or legal value, but also reduces the risk of unfavorable outcomes in litigation. Defensible disposition lowers the cost of e-discovery because the volumes of information to be reviewed are reduced, which leads to significant savings. That is money that could go straight to the bottom line. Research indicates that there are very few organizations that are actually systematically deleting data across all systems, and the goal is never perfection. A more realistic approach is to demonstrate a good faith effort and start deletion processes in the most important systems where the firm can do it in a defensible manner. The email system should be the first one to tackle, as emails are the most requested type of evidence in civil trials because what people put in emails can often incriminate firms.

Information Overload and Inefficiencies

It is not news to anyone in today's digital world that information volume grows exponentially, and most companies often cannot control it. Assuming information is an asset, or at least that is how firms should look at it, when there is too much information, its value starts to decrease. That is not because the intrinsic value goes down, but rather because people cannot find it in a timely manner. According to the survey on the information explosion by the Council of Information Auto-Classification, 50% of companies surveyed stated that they need to re-create business records to run their business because they could not find the original records.[8] It is definitely a waste of company resources to retain information and then, when it cannot be found, spend more resources to recreate it.

Many firms are still struggling to classify electronic records and formally manage them. Every firm has legacy systems that have large volumes of unclassified legacy data of which most is never touched again shortly after creation. Over the years the problem of unmanaged information has gotten worse. As organizations have been faced with massive amounts of unstructured data, many have chosen to adopt a "save–everything" mentality that can lead to severe repercussions, such as: the inability to locate business information, increased storage costs, soaring litigation and e-discovery costs, and buried intellectual property, trade secrets, personally identifiable information, and regulated content. In such environments, sound information governance becomes a necessity to begin addressing the "information problem".

RIM Standards and Best Practices

Records management standards must be considered when developing RIM policy. Standards help assure a certain level of quality of products/software, interoperability between different vendor platforms, support uniform implementation of RIM requirements across different systems, and can represent best practice recommendation reflecting international consensus of experts. Some key industry standards applicable to U.S. firms are ISO 15489 and DoD 5015.2 for records management, ISO 23081-1 for records metadata, ISO/FDIS 18829 for assessing ECM/EDRM implementations' trustworthiness, and ISO/IEC 27001 and 27002 for information security controls.

Best practices in RIM are evolving and expanding, and those that apply to a particular organization may vary based on the organization's culture, risk appetite, and history of regulatory or other issues. Some widely applicable best practices are mentioned throughout this paper, such as an enterprise-wide RIM program scope, executive sponsorship (which is crucial), the importance of cross-functional stakeholders to implement RIM initiatives, and defensible disposition of records and information that no longer have value. Other best practices will be mentioned throughout the remainder of this paper.

Lacking or Ineffective RIM Practices

Failure to implement and enforce sound information management practices can lead to vulnerabilities that can have severe consequences. The well-known case of Edward Snowden, who stole confidential U.S. National Security Agency information in 2013, is a perfect example of failure of information management. Also, Ford Motor Company lost an estimated $50 to $100 million dollars as a result of the theft of intellectual property documents by one of its own employees.

Schemes to compromise or steal information can be very deceptive and elaborate if proper information governance controls are not in place. As an example: during a fraudulent medical leave, an employee at Accenture, a global consulting firm, was allowed access to the company's knowledge base containing proposals, expert reports, cost-estimating guidelines, and case studies. The employee then went to work for a direct competitor and continued to download the confidential information from Accenture because the remote access to Accenture's internal network was not terminated. In the end, Accenture lost close to 1,000 documents. This event could have been prevented if Accenture had proper information governance controls, such as monitoring and analytics to detect an unusual amount of downloads (especially for an employee on medical leave), and information rights management technology to secure the documents directly, even after the employee left the company.[9]

Information Security Breaches

Breaches of personal information that reveal failures in privacy protections stemming from failure of aging hardware, human negligence, phishing attacks, ransomware attacks, or faulty software, are announced in the news almost every day. During regulatory exams in 2018

the OCC discovered weaknesses in controls and governance related to information security within banks. “We’re finding weaknesses in patch management, and too many institutions not having adequate assessment and testing,” said Robert Phelps, director for critical infrastructure policy at the OCC. “Access management is another area of flaws, so when bad guys do exploit a patch, they can move within the environment. Access management is the second area where we’re finding too many weaknesses.”[10] The headline data breach of 2017 was the cyberattack on credit reporting agency Equifax which compromised personal information including names, social security numbers, driver’s license numbers, credit card numbers and personal documents, relating to an estimated 145 million individuals. The breach occurred in May and was due to Equifax’s failure to install patches that were released in March.

Even though financial institutions are some of the primary targets of hackers, historically it has been very difficult to justify the business case for RIM. Part of the challenge is that the firms do not have good tools to calculate the cost of storing too much of unneeded information, and also the benefits of clean, reliable, and accessible information. For all the time and resources invested in models to estimate potential losses from market and credit risks, many firms are unable to measure their exposure to data breaches with the same degree of accuracy. Part of the issue is the non-linear relationship between a firm’s safeguards and its likelihood of suffering a loss, as the safeguards are only as good as the weakest link. The unfortunate outcome of this problem is that many institutions only focus on and invest in information management after they have been breached and/or fined by regulators for significant privacy or recordkeeping violations (see Appendix 1 for examples or recordkeeping violations by financial institutions).

RIM professionals need to lead their organizations in taking a proactive approach to information management to help reduce the risk of having too much and/or unnecessary information, while increasing the value of information to meet business objectives. The key to improving the value of information is knowing what information is important, who needs it, where it resides, and finding the most effective methods to get that information to those who need it.

4. Risk Management and RIM

The intense regulatory compliance pressure, coupled with increased volatility and unpredictability in the business environment, mandate that financial institutions not only enhance, but transform, their risk management programs. Firms are turning from responding to a continuous number of new regulatory requirements to focus instead on incorporating risk management into business strategy and on improving operational processes.

According to the Global Risk Management Survey conducted by Deloitte from March 2018 to July 2018, and completed by 94 financial institutions around the world, 90% of respondents reported that their institutions are extremely, or very effective, at managing risk in traditional areas such as markets (92%), liquidity (87%), and credit (89%). However, the survey finds the emerging key risk areas are non-financial in nature. These are led by cybersecurity threats, followed by regulatory and outsourcing (third-party) risks. In addition, survey findings indicate that 67% of respondents named cybersecurity as the risk that would increase the most in importance for their institution over the next 2 years, well ahead of regulatory risk (25%).[11] This is to be expected as the numerous cases of hacking and cyberattacks cost "about $445 billion across all industries in 2016, up 30 percent from three years before," the survey notes.

The same trends are evidenced by a survey published by Risk.net from a series of interviews with chief risk officers, heads of operational risk, and senior practitioners at financial services firms that took place in January and February 2018.[12] Figure 2 presents the top 10 operational risks financial institutions faced in 2018 compared to 2017.

	2018 position	2017 position	Change
IT disruption	1	1*	→
Data compromise	2	1*	→
Regulatory risk	3	2	↓
Theft and fraud	4	9	↑
Outsourcing	5	3	↓
Mis-selling	6	5*	↓
Talent risk	7	new	
Organisational change	8	6	↓
Unauthorised trading	9	5*	↓
Model risk	10	-	↑

**Cyber risk category in 2017 survey was broken down into 3 individual risk categories in 2018 survey to represent more specific areas of concern– IT disruption, data compromise, and theft and fraud. Similarly, conduct risk category in 2017 survey was broken down into mis-selling and unauthorized trading risk categories in 2018.*

Figure 2 – Top 10 Operational Risks for 2018 **Source: Risk.net, February 22, 2018**

As with Deloitte's survey, according to Risk.net 3 out of the top 5 risks in 2018 were: IT disruption, data compromise, and theft and fraud that collectively represented cybersecurity risk as the most challenging non-financial risk, with regulatory and outsourcing (third-party) risks making up the other 2 of the top 5 risks. So what is the role of RIM professionals in mitigating the key risks faced by the financial institutions today?

Cybersecurity Risk

Given the rise of data breaches and their size, such as Target, Anthem, Equifax, Marriott, and cyberattacks by nation states, it is no surprise that information security is a top priority for public and private sectors as well as governments. It is estimated that 60% of the breaches reported by U.S. financial institutions in 2017 were social security numbers, with credit or debit card numbers accounting for 29%. According to data gathered between 2008 and 2017 by ORX News, the majority of the breaches of financial institutions were due to hacking (47%), followed by third-party breaches (19%), employee errors (18%), and malicious actions by employees (16%).[13]

The expression “it is not *if* the breach will happen, it is *when* the breach will happen” has become a fact of life. Financial organizations are among the most targeted by hackers, and the notion that the hackers can be stopped from entering an organization by building strong barriers along the perimeter is no longer convincing. Stopping all attacks is an unattainable goal and firms have to accept that hackers will get in. However, what they find on the inside when they do, and how much damage they can cause, is what RIM professionals can and should control. The job of RIM professionals is to help Chief Information Security Officers minimize the risk of information, and that is a goal that can be accomplished.

Most firms have terabytes of sensitive information that do not need to be retained for legal, regulatory, or business purposes and can be deleted. However, doing so is one of the greatest challenges most financial services institutions face. The biggest obstacle in implementing defensible disposition processes is lack of alignment between records management and data governance policies, user expectations, litigation processes, and technology capabilities. Every organization has a different risk appetite, and some take a very conservative approach to information disposition while others are more progressive. However, regardless of the risk appetite the following steps can be undertaken in any organization:

1. **Assess and address records** – Start with implementing defensible disposition processes on records that are stored in physical archives and electronic records management systems. This is the easiest task to tackle since all content in those systems are records.
    a. Review legal holds and determine if any of them have already been terminated but records associated with those holds never removed from hold. This may not be an easy task if the firm has not been keeping a good inventory of legal holds and records and information associated with the holds. Once legal holds have been cleaned up, more records will become eligible for disposition.
    b. Use the retention schedule as the guide to apply retention periods to records and destroy any that have met their retention requirements, provided they are not part of active legal holds.
2. **Assess and address non-records** – Once record keeping systems have been cleaned up, determine other locations of sensitive information that are unmanaged or repositories, like personal and shared network drives, and SharePoint, that might store records and

non-records. This task is a lot harder to implement as the proliferation of information, especially non-records such as duplicates and transient documents, is growing faster and faster. Automated tools like file analytics software to evaluate documents on network drives or SharePoint are required to make this task manageable, as it would be unrealistic to review millions of documents manually. There are many file analytics tools on the market and one can be selected to fit the firm's budget and maturity level. The following are the steps to address information on network drives:

a. Assess and address Redundant, Obsolete, and Trivial (ROT) data - Finding and addressing ROT data is the easiest step and requires the least amount of setup from a file analytics tool. To address ROT, the tool only needs to interrogate file metadata, i.e. file name, file type, file size, file date, and date modified. It does not need to open the file and interrogate the contents. Because of that the scans are faster with speeds close to 1 million documents per hour. Typically, about 30 – 80% of files on network drives are ROT, so doing this analysis first takes a big chunk of documents off the table for analysis in subsequent, more complex steps. Once ROT is identified, it can be either quarantined for some time in a dedicated repository, by leaving it in place, or removing access to it, or it can be deleted right away.
b. Assess and address sensitive data – Finding and assessing documents containing sensitive data, such as personally identifiable information, protected health information, payment card information, and intellectual property, requires more sophisticated analysis by the analytics software. If 30 - 80% of data identified as ROT has already been eliminated, finding and addressing sensitive data becomes much less resource- and time-consuming. Rules must be set up using out-of-the-box and customizable rules for identifying sensitive information using pattern matching, i.e. ###-##-### for social security number. This process will take time to set up and may take many iterations until RIM professionals are comfortable with the outcomes.
c. Assess and address records – Finding and addressing records on network drives requires the most sophistication from the file analytics software, and some firms may not be comfortable entrusting their records identification to an automated

tool. Additionally, if the firm allows storage of regulated records on network drives, those repositories are likely not equipped to retain records in a manner prescribed by the regulations and would have to be moved into one of the compliant electronic records management systems. For non-regulated records, there could be alternate ways to manage retention should the firm decide to keep them on network drives or SharePoint. One way is to organize records in folders by record type so that retention could be applied on a folder level based on the retention period defined for each record type in the retention schedule. Another way is to organize records by department, such as Finance, and apply the longest retention period for all records belonging to that department, e.g.: if a department has 1-, 5- and 10-year retention periods for its records, make them all 10 years and classify all the documents as one type – Finance records. The goal is to get as few categories or folders as possible to make the deletion process easier.[14] If a firm's policy is not to store records on network drives, and it can be safely assumed that the only documents found on network drives are non-records, then one "blanket" retention period can be applied to all documents on the network drive, such as 3 years after last modified. What the "blanket" retention period should be is a decision each firm has to make based on their risk appetite and business needs. Some financial institutions choose 3 years, but most opt for a longer period such as 7, 8 or 10 years.

When first implementing defensible disposition processes, it is important to obtain the support of the Legal and Compliance stakeholders to make sure they are fully in support. Some organizations, especially at the start of disposition implementation efforts, will require sign-offs from business owners before any deletion of records can happen. This is understandable because changing the culture of "keeping everything forever" takes time. To make the transition to the culture of defensible disposition, it is recommended to start slow with small volumes before moving to larger volumes of information. The goal, however, is to get to the automated disposition state when no additional authorizations from the business owners or Legal and Compliance are required, and the records are destroyed via automated processes as soon as, or soon after, they reach their retention

requirements. When it comes to non-records, the best practice is to perform disposition on a periodic basis, such as annually.

It is important to keep metrics on volumes of records and non-records deleted and calculate cost savings realized through disposition, such as physical storage cost savings, reduced infrastructure and system maintenance expenses, reduced staff costs, etc., and report to RIM Management and RIM oversight board(s) as it will help make the case for future RIM initiatives that require funding. The key is to make defensible disposition a repeatable ongoing process, not a one-time initiative.

By implementing defensible disposition processes, RIM professionals can minimize the amount of sensitive information being exposed in a data breach, thereby reducing financial and reputational damages to their firm caused by the breach. In addition, defensible disposition enables ethical and responsible business practices by protecting consumers who entrusted their personal information to the firm.

Regulatory Risk

The constantly changing regulatory landscape is one of the biggest operational risks for financial institutions today. The regulators in the U.S. and around the world are increasing their focus on risk management, cybersecurity, consumer data protection and privacy, conduct and culture, and financial crimes. Regulators continue to conduct exams of financial institutions to assess how firms are coping with those challenges, and issue findings about improving risk management and governance practices, often reaching levels of enforcement actions and fines (see Appendix 1 for some recent fines issued to financial institutions).

While the pace of regulatory changes in the wake of the Great Recession seems to have slowed down, financial services institutions are preparing for a number of regulatory requirements that are still to be finalized, and assessing the full implications of implementing those that have recently been finalized. RIM professionals need to stay abreast of regulatory developments by collaborating closely with the Business, Legal, and Compliance stakeholders in their organizations to be able to adequately respond to the changes and incorporate them into the RIM processes. According to KPMG, financial services organizations will face the following 10 key regulatory challenges in 2019, shown in Figure 3.[15]

Figure 3 – Ten Key Regulatory Challenges for 2019 **Source: KPMG, December 4, 2018**

Every one of the key regulatory challenges has implications on RIM. Table 1 describes the likely actions RIM professionals need to take, if they have not already, to help their firms address the regulatory challenges in a proactive manner.

Table 1 – Ten Key Regulatory Challenges for 2019 and Actions for RIM Professionals

Key Regulatory Challenge	Actions for RIM Professionals
Divergent Regulation Revisions of existing federal regulations, new state legislation and regulation, global divergence in regulation, implications of jurisdictional policies, including sanctions and tariffs, nonbank supervision	• On periodic basis refresh the inventory of federal and state recordkeeping regulations applicable to the type of financial institution • Where multiple jurisdictional requirements exist, determine the precedence of various rules to ensure that correct retention requirements are applied to record categories/types • Map record categories/types in the retention schedule to specific regulatory citations for ease of determining the drivers behind retention requirements and maintaining future changes • Pay attention to non-bank regulations, such as affecting FinTech companies, that provide payment processing and data aggregation services, but do not fall under prudential bank supervision • Formalize the process for organized, adequate, and timely response to regulatory inquiries and exams, and internal or external audits
Risk Governance and Controls Strengthening risk management practices, third party risk management, IT and data governance	• Determine if supervisory controls for RIM, especially for high-risk regulatory requirements, such as for broker-dealers, are functioning effectively • Engage with Business, IT, Operational Risk, Compliance, Legal, Data Governance, Data Privacy, and Information Security stakeholders to evaluate ways to enhance supervisory controls in support of stronger risk management and compliance culture enterprise-wide • Build change management components into the RIM program • Further integrate third-party risk management with RIM for improved governance and oversight

Key Regulatory Challenge	Actions for RIM Professionals
Data Privacy Federal standards being considered, state laws being enacted, global nature of GDPR	• In collaboration with Data Privacy, Information Security, and Data Governance, inventory the personal data collected, processed, stored, and shared • Map personal data to records, taxonomy, and storage locations identifying "golden source" vs. duplicate data/locations • Link data privacy programs with RIM, Cybersecurity, and Data Classification programs • Implement a RIM employee training program that incorporates data privacy and cybersecurity elements to reinforce awareness and employee responsibilities
Compliance Processes Increased governance expectations for the board of directors, converging compliance risks and controls, renewed focus on trade reporting, SEC and CFTC exam focus on record retention	• Identify and continuously refine RIM metrics to provide more valuable and consistent RIM risk information to the RIM oversight board(s) • Understand the regulatory change management process at the firm, and ensure that regulations related to recordkeeping requirements are in scope and RIM staff is included • Understand the "three lines of defense" model for management records and information for more streamlined compliance, improved risk management, and enhanced first line ownership of compliance risks by record owners • Gather and maintain an inventory of all regulated records mapped to regulatory citations, analyze if repositories that store regulated records comply with regulatory recordkeeping requirements and, where gaps exist, develop remediation plans to achieve compliance
Credit Management Eased underwriting standards and increased credit risk, credit risk management, better internal controls and process infrastructure	• The OCC and the Federal Reserve have each identified credit risk as its top supervisory priority for 2019, which will result in additional risk-related records to be retained in order to comply with the supervisory requirements • New risk control-related records would need to be identified and mapped to appropriate regulations to evidence not only that the controls are in place, but that they are actually working and tested periodically for effectiveness

Key Regulatory Challenge	Actions for RIM Professionals
Cybersecurity National Cyber Strategy released by the federal government, multiple federal financial services regulators have cyber requirements, emergence of state cybersecurity regulations	• Understand relevant cybersecurity laws and regulations, such as NYDFS 23 NYCCR 500 Cybersecurity regulation that mandates periodic disposition of non-public information, and assess the impact on RIM • In collaboration with Data Governance and Information Security, consistently implement information management policies for records, non-records and data, and ensure consistent enforcement • Participate in data-breach response table-top exercises and provide input to the incident-response planning • Participate in incident response by addressing records and information related inquiries • Implement a RIM employee training program that incorporates data privacy and cybersecurity elements to reinforce awareness and employee responsibilities
Ethics and Conduct Broad definition of conduct risk by various regulators, evaluation of the effectiveness of board of directors and senior management charged with overseeing conduct	• Be aware of new technologies/tools being introduced to enhance surveillance, monitoring, and reporting of employee conduct, as those systems may contain records and must comply with regulatory recordkeeping requirements, or need to have proper information lifecycle management controls
Consumer Protections Greater control over collection, use, and retention of personal information, expectations for a "personalized experience", regulatory changes to consumer protection laws	• In collaboration with Data Privacy, Information Security and Data Governance, inventory the personal data collected, processed, stored, and shared • Map personal data to records and storage locations identifying "golden source" vs. duplicate data/locations • Implement information lifecycle management capabilities that support individual rights, such as defensible disposition
Financial Crimes Development of data analytics that are aggregated across various types of financial crimes, further automation of financial crimes efforts	• The firms have been investing a growing amount of costs into technology and staffing for anti-financial crime and know your customer (KYC) functions in the last few years. Those new systems may contain records and must comply with regulatory recordkeeping requirements, or need to have proper information lifecycle management controls • Help prevent, detect, or respond to financial crimes through sound recordkeeping practices enterprise-wide

Key Regulatory Challenge	Actions for RIM Professionals
Capital and Liquidity Higher SIFI threshold and new asset categories, new liquidity requirements, continued testing/supervisory reviews	• Recent capital- and liquidity-related regulatory requirements resulted in raised asset threshold and new asset categories which reduced the regulatory burden for most firms. However, some firms may find themselves forced to choose between growing their asset base and thereby increasing regulatory burden, or sacrificing growth to remain below regulatory threshold of a new tier of requirements. RIM professionals need to know the asset category the firm falls under to ensure proper regulatory compliance.

Outsourcing (Third-party) Risk

Outsourcing (third-party) risk is the third biggest operational risk faced by the firms resulting from the growing reliance on external service providers for everything from online transaction processing to extra network capacity. The number of external service providers some larger financial institutions use can be in the thousands and requires a rigorous and consistent third-party risk management framework. Being able to monitor the way the vendors do business and protect the firm's data and intellectual property is a constant area of concern. The large retailer Target was breached through a heating and air conditioning contractor, which was a wake-up call to organizations in all industries to review and tighten their vendor management practices.

A big concern in financial services is the growing use of external cloud services which involves on-demand access to a shared pool of computing resources, such as servers and applications. IT and the business are putting pressure on RIM professionals to move records storage to the cloud because of the obvious benefits of infrastructure cost savings, which in some cases can lead to lower prices to the firm's clients. Nevertheless, the financial sector has been slow in adopting cloud computing for regulated record storage because of the compliance burdens with the recordkeeping rules that cloud solutions must meet, especially those related to the retention of broker-dealer records.

Regulated Record Storage in the Cloud

According to SEA 17a-4(f), broker-dealer firms are required, among other things, to preserve certain records in a non-erasable, non-rewritable format, otherwise known as WORM. In recent years regulators have been focusing on this topic, as illustrated by the almost $30 million in fines that FINRA issued between 2016 and 2017 for books and records violations. At the same time, as many firms have been working to bring all of their regulated records into compliance, they have also experienced the increasing presence of cloud solutions aimed to reduce, if not eliminate entirely, a firm's physical technology infrastructure. These parallel developments lead to the question: Can WORM storage be achieved in the cloud?

There are two ways in which firms can use cloud solutions for regulated record storage. The most common solution is software-as-a-service ("SaaS") cloud solution where a firm engages a cloud provider to supply an application service. The firm then configures its existing business applications to archive regulated records to the provider's system rather than its own internal system. The solution includes an application, usually web-based, which the firm will use to access its regulated records. One example of a SaaS solution that is getting a lot of traction in financial services is an electronic communications archiving system, such as one provided by vendors like Global Relay, Smarsh, or ZL Technologies. An emerging alternative to SaaS is an infrastructure-as-a-service ("IaaS") cloud solution where the firm engages a cloud provider to supply infrastructure services onto which its regulated records are written and retained compliantly. The firm itself is responsible for providing and maintaining its own records management application, either custom-developed or off-the-shelf, that runs on IaaS resources purchased from the cloud provider.

There are multiple SaaS and IaaS vendors on the market that claim to comply with SEA 17a-4(f), however, the use of such services does not relieve the firms of their obligations related to FINRA supervisory Rule 3110 and guidance in FINRA Notice 11-14 to ensure that whatever platform they select is correctly configured and able to be compliant. The firms should also not forget other requirements of SEA 17a-4(f) beyond WORM (i.e. submitting 90-day notification to the regulator, duplicate WORM storage, D3P) which the firms must also meet to be in compliance with the SEA rule (refer to Section 3 – Drivers for RIM in Financial Services for a full list of SEA 17a-4(f) requirements).

While some of the leading IaaS providers, such Amazon, Microsoft, Google, and IBM, are likely to use security technology that is at least as advanced or probably more advanced as those of their financial services customers thanks to their technical expertise and economies of scale, the records management related configurations of their products still need to be assessed by the RIM professionals with a great deal of scrutiny. Figure 4 presents a cloud storage compliance assessment of the major IaaS providers by Cohasset Associates. The assessment illustrates the fundamental RIM requirements and how they are met by the cloud providers which RIM professionals must understand in order to ensure proper implementation and regulatory compliance.

	Immutability	*Retention*	*Legal Holds*	*Disposition*
amazon web services™	Yes, *during and after* Retention or Hold	Time-based	Object Level (S3) Bucket Level (Glacier)	Lifecycle action
Microsoft Azure Azure Blob Storage	Yes, *during and after* Retention or Hold	Time-based	Bucket Level	Lifecycle action
Google Cloud Storage	Yes, *during and after* Retention or Hold	Time or Event-based	Object Level	Lifecycle action
IBM Cloud Object Storage	Yes, *during* Retention or Hold	Time or Event-based	Object Level	Lifecycle action

Figure 4 – Cloud Storage Compliance Assessment **Source: Cohasset Associates, January 31, 2019**

While SEA 17a-4(i) allows broker-dealer firms to use "other recordkeeping service on behalf of the member, broker or dealer"[16], it mandates that such third party files a written undertaking with the SEC confirming that the records will be retained in accordance with the rule and made available for examination or production to the regulators. Additionally, FINRA issued interpretive guidance 18-31 where it clarified 17a-4(i) and stated that third parties cannot delete broker-dealer's records due to non-payment. The guidance further outlined that "if a service provider deletes or discards broker-dealer records in a manner that is not consistent with the retention requirements of Rule 17a-4, such action would constitute a primary violation of the rule by the broker-dealer and may subject the service provider to secondary liability for causing, or aiding and abetting, the violation."[17] The requirement of written undertaking with the

regulator, and the threat of secondary liability for violating recordkeeping obligations on behalf of the firm, are what deter some of the smaller cloud providers from engaging in regulatory recordkeeping services.

The first steps in implementing a cloud-based solution are to identify the applicable regulatory requirements, define the firm's interpretation of those requirements (sometimes with the help of the outside counsel), and translate those requirements into functional and technical requirements that can be used to drive implementation of the recordkeeping system. This is not just the job of RIM professionals, but rather a collaborative effort between RIM and other stakeholders, such as Legal, Risk, Compliance, Business, IT, and Information Security. Which SaaS or IaaS vendor to choose should be a decision based on several factors, such as the firm's overall technology strategy, risk appetite, and the degree to which the functional requirements can be met by SaaS or IaaS solutions.

When evaluating and selecting cloud providers, firms usually face two challenges. First, the cloud provider may not be able to provide the level of detail about its underlying architecture that a firm needs to have as part of its vendor due diligence. A cloud provider might view that information to be proprietary or reserve the right to change their hardware platform later. Second, the cloud provider and the firm may not align on the definition of WORM itself. Some cloud providers might only protect a customer's data using controls at the level of an application, application programming interface, or administrative console, but advertise WORM capabilities in alignment with regulatory requirements. If the firm defines WORM to require data protection at a hardware level, protected even from the system administrators of the cloud solution, then that cloud solution might not meet the firm's requirements.

Contractual Requirements and Oversight of Third Parties

Once the firm has selected a cloud provider that meets its needs, the next step is to create an agreement with the vendor that addresses all the firm's requirements. The agreement would look different for a provider of a SaaS solution rather than for a provider of an IaaS solution. For example, a SaaS provider might be able to supply D3P services to its customers or help responding to a regulatory record request, while an IaaS provider is unlikely to be able to do so and the firm will have to make other arrangements to meet those requirements. Regardless of the

type of cloud solution, the firm must address core items, such as attestation to regulatory compliance, the ability of the firm to audit and review cloud solution for compliance, etc.

Once a firm makes a decision to outsource records storage to the cloud, making sure proper oversight of the cloud provider is in place becomes a key task of RIM professionals in conjunction with other stakeholders involved in risk management. A firm generally has very little control over cloud providers which introduces data security, regulatory, and business continuity risks. Outsourcing an activity or function to a third party does not relieve a firm of their ultimate responsibility for compliance with all applicable laws and regulations. In the eyes of the regulators, the firm, not the cloud providers, is the one that owns the records and the risk. Therefore, firms need to treat those third-party environments as their own and have appropriate governance and oversight that lays out key processes, such as change management, audits, internal controls, record transmission reconciliation, and mechanisms to adapt to a changing regulatory landscape.

The oversight is even harder, or almost disappears, when a firm's vendors employ subcontractors (fourth parties). One way firms can have some control over fourth parties is to require cloud providers to give notice that they are employing a subcontractor, and give firms the right to approve or terminate that particular service. Another recommendation is that firms clearly stipulate in their contracts with the cloud providers which activities can be subcontracted and require that any subcontractors must fully comply with the obligations placed on the original cloud provider. In addition, the outsourcing contract should also require that the cloud provider notify the firm of any changes to subcontracting arrangements in order for the firm to perform a risk assessment.

A strategy for terminating the relationship with a cloud provider is another hurdle financial institutions must overcome before cloud computing can be more broadly adopted by the industry. Whether the firm wants to pull out of the outsourcing relationship, or should the cloud provider fail, the firm needs to make sure exit plans are documented, understood by appropriate stakeholders, and fully tested. Part of the challenge is that firms do not have the benefit of experience to call upon as there is no precedence of any financial institution to ever exit from a significant public cloud contract.

U.S. regulators recognize that financial institutions are becoming more dependent on cloud services providers to conduct business, and see that as a source of risk. However, unlike the European regulators, such as the European Banking Authority, U.S. regulators have not issued formal guidance on the use of cloud providers by financial institutions. The industry would benefit from such regulatory guidance, as it would outline regulatory expectations for firms outsourcing services to cloud providers around key areas such as access and audit rights, contingency plans, and exit strategies.

Poor third- and fourth-party vendor management leaves firms exposed to the risk of costly data breaches. RIM professionals must be standing members of a third-party risk management process in their organizations to ensure that vendor contracts have the appropriate risk management clauses and provisions for subcontracting, data and record retention, disposition, legal holds, inspection, data transfers, etc., to enable the most control over the data. One way to mitigate third-party risk is through regular audits of cloud providers, whether by firms themselves, pooled audits by several firms, or third-party audits (no irony intended).

In the face of the emerging nonfinancial risks, financial institutions need to re-engineer their risk management programs in order to address these new challenges. The first step is to ensure the firms have the properly trained personnel in the areas of non-financial risk that can build the risk-awareness culture and engage all employees in supporting that culture. An important component of a renewed risk management program should be the implementation of the “three line of defense” risk governance model to eliminate overlapping responsibilities, ensure business lines take ownership of the risks they assume, and have risk management functions to provide oversight. Transforming risk management programs also involves employing the latest technologies, such as cognitive analytics, machine learning, and robotics to reduce costs through automation, building controls directly into processes, and identifying potential risk events in real time.

5. Electronic Communications – Retention and Supervision

Electronic communications (e-communications) is one of the key record categories that RIM professionals at financial organizations need to manage effectively. While 15 years ago emails were the only means of e-communications utilized at workplaces, today firms are witnessing a number of emerging communication technologies being employed in conjunction with email to conduct business as they offer more interactive and effective ways of sharing information with internal and external parties. Such new e-communication technologies include instant messaging, social media, blogs, chat rooms, and websites.

Email

Email has been around the longest and remains to be the main form of business communication and the major area of attention for RIM professionals at any firm. Employees use email all day, sometimes mixing business and personal use. A portion of emails may be declared as records as they may support business transactions, decisions, or activity, have legal ramifications or historic value, or may be related to communications with clients. Some emails contain records, such as reports, statements, and trade confirmations. Email systems can be compromised through cyberattacks, employees sending work email to and from their personal accounts, and other employee errors resulting from negligent or malicious behavior that can lead to damaging consequences for the firms. All these reasons make it critical for firms to implement proper governance controls around email communications.

The key to managing email is having adequate email and e-communication policies that are regularly updated to keep up with increasingly sophisticated users who are able to find ways to go around company policies on email use. Policies must be realistic and technology agnostic. The policies should include a list of permissible forms of e-communication, clearly state if certain forms may only be used for communications between employees of the firm (versus forms of communication that may also be used for communications with the public), explain the potential consequences of non-compliance, and state that there should be no expectation of privacy when using corporate communication channels.

Email retention is mainly a legal issue. Employees often say inappropriate or incriminating things in emails, and many times email messages serve as smoking guns in

lawsuits and investigations. Emails can play an important role in reconstructing events and motives for legal purposes. Consequently, email is the most requested type of evidence in civil litigation today. To minimize the risk of employees altering email contents and metadata, and deleting emails to "cover their tracks," most firms decide to capture and archive automatically (journal) in real time all incoming and outgoing emails.

Given the enormous volume of email exchanged in the course of business, most email communications do not rise to the level of records. Since emails represent a significant legal risk in case of litigation, firms should keep them for as short a period of time as possible, typically anywhere between 90 days and 3 years. A small number of emails are considered records and need to be managed in accordance with regulatory and legal requirements. Employees need to classify those emails by moving them to predefined folders that have the appropriate retention periods applied to them, which are separate from the retention period for emails that are non-records. Another, and perhaps better approach to handle emails that are records, is to mandate that employees archive those emails into a company-approved enterprise content management (ECM) system, or another form of electronic record repository where other business records are stored. The latter approach would also accommodate for email records that are event-based, such as client-related communications, and rely on a closure event, such as the end of client relationship, to trigger the start of the retention period.

Like any other type of e-communications, emails are subject to FINRA Rule 3110 that mandates firms have supervisory controls over email communications, including surveillance. FINRA Regulatory Notice 07-59 – Supervision of Electronic Communications provides useful guidance for firms to consider when developing supervisory controls for e-communications that are reasonably designed to achieve compliance with SEC and FINRA rules. According to the guidance, firms can take a risk-based approach and have the flexibility to design supervisory review process for internal and external communications that is appropriate to the firms' business model (e.g. size, structure, customer base, and product mix). Thus, the firms may consider to use lexicon-based reviews of e-communications (those based on sensitive words or phrases, the presence of which may signal problematic communication), or choose to use a reasonable percentage sampling technique, whereby some percentage of the e-communications is reviewed, or a combination of the two methods. The frequency of e-communications review may

vary depending on the business model. Regardless of the review method selected, the firms must evidence the review, whether electronically or on paper, and be able to reasonably demonstrate that such reviews were conducted. Additionally, if the firms allow employees to communicate with clients using Internet-based email systems (e.g. Gmail, Yahoo, etc.) or third-party communication platforms (e.g. Bloomberg, Reuters, etc.), the firms are required to supervise and retain those communications.

Instant Messaging

Instant messaging (IM) use is not widely adopted by financial services yet, although more and more business cases arise for the use of IM for conducting business, such as making and confirming appointments with clients, and answering questions related to products, etc. The line between personal and business communications can be blurred very easily when it comes to IM. As with emails, the first step in governing IM is the creation of an IM policy that would define acceptable use and the consequences of violations of policy.

If the use of IM for conducting business is permitted by the firm, unaltered archiving of IM messages, together with associated metadata, should be implemented in real time, and an appropriate e-communications retention policy should be applied to meet the requirements of SEA Rules 17a-3 and 17a-4 and FINRA Rule 4511. IM messages, like emails, are susceptible to cyberattacks and employees should be trained to not click on links embedded in IMs, or open IM attachments, to prevent initiating malicious executable files. IM policy should be reviewed at least annually and updated to reflect the latest developments. Monitoring of IM conversations needs to be in place and communications containing certain keywords can be blocked. The use of a standard disclaimer inserted in all IM sessions can remind employees of appropriate IM use, that all chat sessions are being monitored and archived, and can be used in court.

Social Media, Blogs, and Chat Rooms

Blogs and chat rooms are very similar in nature to social media communications and, therefore, the social media retention and supervision requirements described below will equally apply to blogs and chat rooms.

Compared to conventional marketing tools, such as advertising and direct marketing, social media offers a number of distinct benefits, such as the following:

- It is free or relatively inexpensive.
- It is interactive, providing the means to communicate one-to-one as well as one-to-many.
- It offers immediate, direct feedback from the target market.
- It is adaptable and can be readily refined to promote ongoing success.

Despite the benefits, the adoption of social media has been challenging for financial services firms. Some of the key reasons are regulatory. SEC and FINRA impose strict guidelines on the use of all electronic communications including social media, demanding careful oversight of online communications and activities to ensure that advisors and brokers are not using social media channels inappropriately and without retaining records. Firms also raise concerns about the risks of data leakage, malware, and viruses propagated through these popular channels. New technologies have emerged to address regulatory and security challenges, but firms are still slow to adopt social media within their distributed teams as a means to reach out to clients.

Rule 17a-4 prescribes retention requirements for all types of broker-dealer communications relating to its "business as such", including social media. FINRA Rule 2210, which governs communications with the public, defined three communication categories: 1) correspondence, 2) retail communications, and 3) institutional communications (see Section 3 – Drivers for RIM in Financial Services for additional information on Rule 2210). Two categories that relate to social media are correspondence and retail communications. Communications that formerly qualified as "advertisements" and "sales literature" generally now fall under the definition of retail communications. FINRA Regulatory Notices 10-06 and 11-39 are key pieces of guidance on the use of social media for advertising purposes.

Regulatory Notice 10-06 states that static content is generally accessible to all visitors and usually remains posted until it is removed by the firm. Examples of static content include profile, background, or wall information. A registered principal of the firm must approve all static content on a page before it is posted or before it is changed, and the record of approval must be captured as well. Interactive content is considered non-static. Examples of interactive content include Facebook posts, tweets, and LinkedIn status updates. These real-time

communications do not require approval by a registered principal prior to use. However, both static and interactive content are subject to recordkeeping rules and must be supervised. The notice also states that generally, posts by clients or third-parties on a firm's social media sites do not constitute communications with public under FINRA Rule 2210 unless the firm or associate person has 1) paid for or been involved in the preparation of the content (which FINRA would deem to be "entanglement"), or 2) explicitly or implicitly endorsed or approved the content (which FINRA would deem to be "adoption"). If the firm has adopted or has become entangled with third-party site's content, the firm is responsible under the communications rules for content on a linked third-party site, including retention and supervision. The notice also states that a firm may not establish a link to any third-party site that the firm knows or has reason to know contains false or misleading content.

In its Regulatory Notice 11-39, FINRA clarifies the requirements of SEA Rule 17a-4 and outlines that the content of communication is determinative, not the communication channel. Firms must retain retrievable records of business-related communications made through social media, regardless of the type of device or technology, or whether they were made by firm-issued or personal devices. In order to retain all business-related communications, firms may not use communications devices or technologies that automatically erase information.

According to FINRA Rule 3110, firms must have written supervisory procedures in place to supervise communications and periodically monitor compliance. FINRA examiners typically are interested in the types of written supervisory procedures the firms have adopted to address social media. Of particular interest to regulators are policies on the acceptable use of social media channels, the differences between business and personal communications, third-party communications posted to a social media site, disciplinary action for social media use, retention of social media, and the process for handling customer complaints. In addition, regulators are also interested in seeing the documented procedures firms have in place to implement the policies, and evidence that those procedures are being followed. It is recommended that firms use a risk-based approach to determine the frequency of supervisory review. There are several e-communication surveillance tools available to assist with communication review.

Social media is no different from other forms of electronic communications in that it is discoverable during litigation. Like with email, people may use social media to vent about a bad

day at work or expose information that is not meant for public consumption, not realizing that their message can damage the firm's reputation and alienate coworkers or clients. Two of the biggest issues of social media use at the firms come from the lack of an adequate social media policy and employee use of social media channels. Firms must provide training to all employees on all relevant policies and procedures to ensure awareness and compliance with the policies.

RIM professionals must ensure that their firms adhere to the social media recordkeeping rules. Social media sites such as Facebook, offer no native archiving functionality, making it difficult for the firms to comply with recordkeeping obligations. This mandates that firms invest in third-party e-communications archiving solutions that provide preferably a unified interface to manage all types of communications including email, IM, social media, etc., preserving the native format of communications with the ability to review and download messages, demonstrate a full audit trail, apply retention period, legal holds, and perform defensible disposition.

Websites

Publicly available websites are considered retail communications under FINRA Rule 2210 similar to social media, which means that firms must have policies and procedures in place for review, approval and recordkeeping of their website content. Recordkeeping requirements for broker-dealers are defined in SEA 17a-4. In addition, websites are subject to the same supervisory rules as social media communications prescribed by FINRA Rule 3110. Most ECM products offer a web content management module that can archive website content. Firms may also choose other solutions on the market that are specifically geared toward compliant archival of website content and may include content creation, approval, publishing, and archiving all as part of one product.

6. Industry Trends and Impact on RIM

Emerging e-communications technologies is just one example of new technologies that will continue to impact financial services. Firms are beginning to use a wide variety of other new technologies (described later in this Section) that reflect industry trends and will shape the way firms do business in the future. Many firms are undergoing a digital transformation as an increasing number of transactions are moving to digital channels, and more and more institutions are introducing digital-only entities to provide lending, investing, and specialty services. The focus is on gaining operational efficiencies to provide innovative personalized customer experiences while increasing the information value to both the firm and the customer. Some of the new technologies will have a direct impact on RIM, while others will require RIM professionals to be on the look-out for any potential impacts in the future as technologies mature and get more widely adopted by the firms.

Digital-Only Banks

Digital-only banks are a legitimate competitive threat that needs to be acknowledged. There are three main reasons why contemporary digital-only banks pose an immediate threat to their traditional peers, which highlight the areas that firms need to focus on and invest in to keep pace.

First, digital-only banks are agile and apply resources in the right places. They are technology- and mobile-first, so their research and development mentality and rate of churning out new features and functionality for their customers are innately different. Updates do not have to be developed for and rolled out across multitudes of legacy infrastructure, so they can be more frequent, seamless, and innovative. Being mobile-first also provides the distinct advantage of built-in security mechanisms like two-factor authentication, biometric sensors, encryption, and even fraud detection through behavioral analysis. Many mobile features and security upgrades are one of the last things that traditional banks get around to, which clashes with a recent PwC survey that found nearly half of consumers now rely on mobile and/or online as their primary banking channels[18]. In addition, digital-only banks require fewer employees, less real estate and in-branch hardware, and other overhead, which translates into more financial resources being invested directly into improving technology and the customer experience.

Second, customer service is in their core. Whereas traditional financial institutions have been cited at some point for poor customer service, digital-only banks were born in an age of immediacy, customer choice, and an expectation for exceptional customer service. They tend to not have as many one-off fees tacked on to their services and typically maintain multiple channels for customer service. Part of a customer-first approach is manifested in the fact that digital onboarding is a must for digital-only banks which, when combined with their technology-first mentality, make them pros at it long before traditional banks catch on.

Third, branches only serve a purpose if properly capitalized upon. In the same way that digital onboarding is becoming more popular or even preferred, consumers want to take control of their banking experience through self-service. Younger users do not need the same high-touch treatment that those from older generations do. That is not to say that traditional branches do not serve a purpose. They do, but only if they are leveraged in the right way. In order to keep pace with their digital-only competitors, traditional banks must consider modernizing their in-branch technology with the likes of self-service kiosks, biometric authentication, and instant card issuance to make branches an appealing, effective, seamless, and secure experience.

The cost of operating a branch is high, which makes return on assets significantly stronger for branchless entities. With the high cost of a traditional branch network and the increasing number of transactions moving to digital channels, more and more traditional financial institutions are introducing digital-only entities. Some of the firms that will move in this direction will do so to protect their current customer base, while others will be trying to expand or generate market share. The challenge will be to determine the right mix of physical and digital footprint in 2019 and beyond. Figure 5 shows four formats for physical branches incorporating digital banking solutions developed by McKinsey & Company.

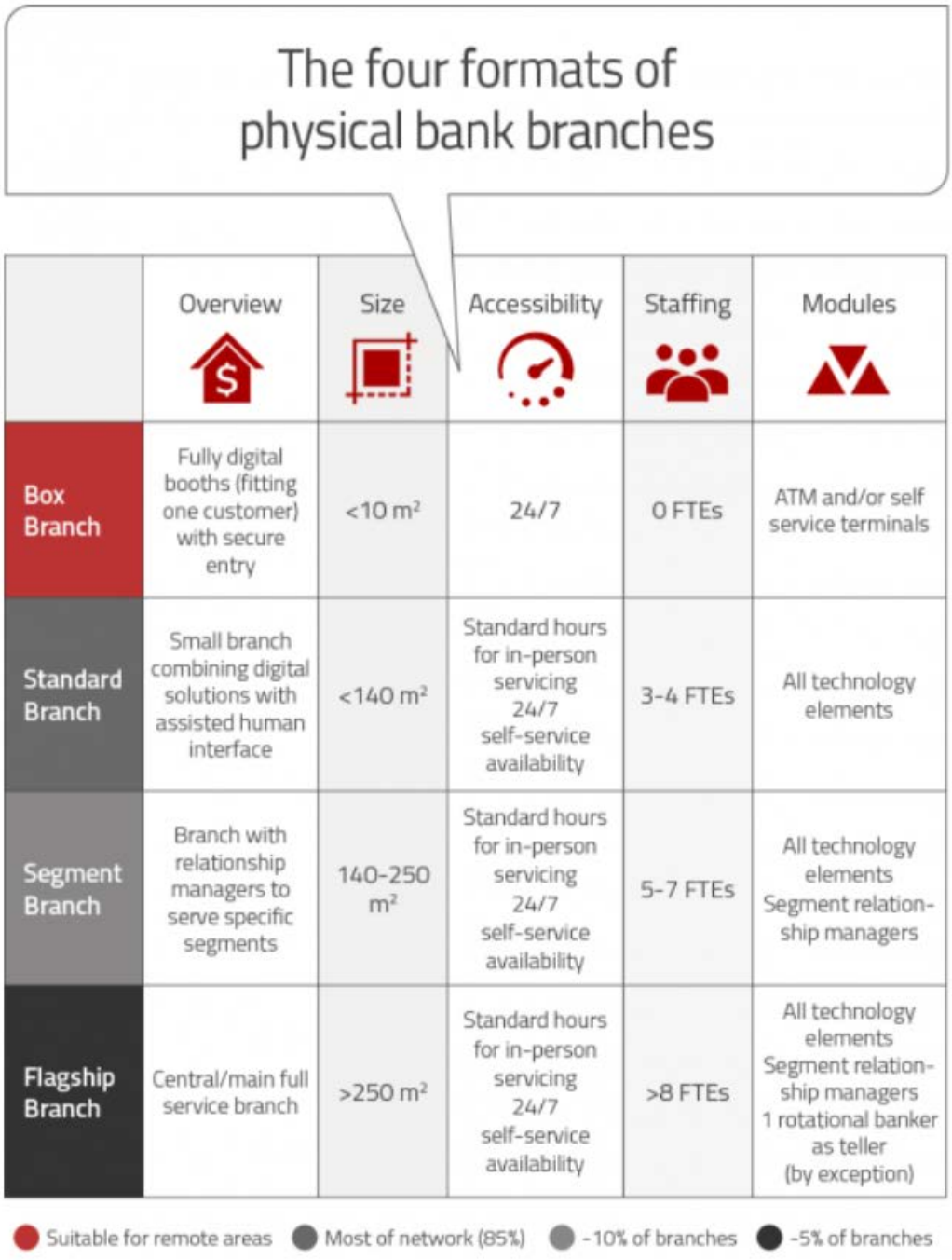

Figure 5 – The Four Formats of Physical Bank Branches **Source: McKinsey & Company, August, 2018**

The digital-only trend in today's financial services sector does not appear to materially affect RIM because the only thing that is changing is the delivery channel for products and services to customers. The system of record that generates and processes transactions in the

back-end remains the same. This means that if the mechanism to capture and compliantly retain records has been put in place for traditional channels such as physical branches, ATMs, and call centers, then the same would be leveraged for digital-only entities. However, if new records are being created that are unique to the digital-only channels, those records must be captured and retained as per legal and regulatory requirements and RIM policy.

FinTech

Financial technology (FinTech) firms are the new entrants into the financial services market that compete with the traditional financial services institutions. Many FinTech firms started out as providers of technology solutions to traditional banks offering products that record, monitor, and report transactions. Other FinTech firms have no previous track record in financial services but have already established a dominant position in their respective industries. They have been quick to leverage part of the financial market subject to lighter regulation such as payments facilitation, and platforms that connect buyers and sellers of financial services such as loans and insurance. They have been able to build market share without having to bear the same costly operational and regulatory burdens as full-service financial institutions.

The FinTech sector faces difficulties within the complex and often overlapping U.S. regulatory framework. FinTech firms have long pushed for national bank charters to let them operate nationwide without needing licenses in every state, a process that can impede growth and increase costs. Over the past several years, the OCC has been exploring its role in the Fintech space and introducing several innovation initiatives. On July 31, 2018, the OCC announced that it would begin accepting applications for special purpose national bank (SPNB) charters from "non-depository" FinTech firms who are engaged in banking. The decision followed the U.S. Treasury's endorsement of regulatory "sandboxes" for FinTech firms, a practice popular with foreign regulators, such as the UK Financial Conduct Authority (FCA). Sandboxes are facilities or innovation hubs that enable firms to test out new services in a safe environment while identifying potential risks. In the announcement from the OCC, Comptroller Joseph Otting said "Providing a path for FinTech companies to become national banks can make the federal banking system stronger by promoting economic growth and opportunity, modernization and innovation, and competition. It also provides consumers greater choice, can promote financial inclusion, and creates a more level playing field for financial services competition." [19]

Similar to traditional banks, the OCC charter for FinTech firms requires them to have a resolution plan in place, as well as requirements regarding capital levels, liquidity, risk management, corporate governance, and long-term business plans. For smaller FinTech firms that are used to operating with minimal constraints, the OCC's charter requirements might be considered a step too far as they would not want, nor could meet, all the requirements. Among companies that might see value in obtaining a national charter, experts cite innovative payment companies, online lending firms, and cryptocurrency exchanges.

As learned from the history of the U.S. financial system, here again several state regulators, including the Conference of State Bank Supervisors (CSBS) and the NYDFS, disagreed with federal regulators over the OCC's decision. Maria T. Vullo, superintendent of the NYDFS noted that "the national charter will impose an entirely unjustified federal scheme on an already fully functional and deeply rooted state regulatory landscape."[20] CSBC and NYDFS have already sued the federal government to void its decision to grant national bank charters to FinTech companies, saying it was unconstitutional and puts consumers and taxpayers at risk. As a result, FinTech firms might be cautious about applying for the OCC license while legal challenges remain unsolved.

RegTech

In recent years, in addition to FinTech, the financial services industry has seen a significant growth in emerging regulatory technology (RegTech) solutions designed to meet compliance needs of firms more effectively and efficiently. The rise of the RegTech industry has been shaped by both regulatory developments and technological innovations. According to a report issued by FINRA in September 2018, nearly 20% of financial services firms have implemented some type of RegTech.[21] The most prominent areas where firms have taken advantage of RegTech innovations are surveillance and monitoring, customer identification and anti-money laundering compliance, regulatory intelligence, reporting and risk management, and investor risk assessment.

The area that directly aligns to RIM is regulatory intelligence. It is the area of compliance that focuses on the identification and interpretation of changes to applicable rules and regulations, frequently across multiple jurisdictions, in order to update the firm's compliance

operations, including retention requirements and retention schedules. Compliance and risk practitioners from nearly 800 financial services firms across the world, including banks, brokers, asset managers and insurers, have taken part in the 2018 Cost of Compliance survey conducted by Thomson Reuters, where they found that 66% of firms expect the cost of senior compliance staff to increase, up from 60% in 2017.[22] RIM professionals continue to identify managing and coping with continuing regulatory changes as one of their biggest challenges.

Any RIM professional who has worked in a highly regulated industry like financial services, would attest that manual processes are not only expensive and slow, but unable to provide the degree of regulatory intelligence required to determine which regulations are relevant to their business, and how to avoid compliance gaps. Since the Great Recession, the firms reacted to the surge of new regulations by increasing their compliance staff, but the volume of regulations kept on coming. Just throwing people at the problem - which in itself introduces risks and inefficiencies - does not solve the problem. Technology, on the other hand, can improve operational and commercial efficiencies. RegTech is having a major impact on compliance today with 41% of Thomson Reuters' survey participants expecting to spend more time assessing FinTech and RegTech solutions over the next year, rising to 55% in the global systemically important financial institution (G-SIFI) population. As reported by Bloomberg, investments in regulatory intelligence software can lead to an ROI of 600% or more with a payback period of fewer than three years.[23]

As of the writing of this paper, there are 770+ RegTech startups operating around the world, 70+ of which are regulatory intelligence solutions that continuously monitor regulatory change, alert RIM and compliance professionals of the changes that impact the recordkeeping requirements, and enable rapid remediation of policies, retention schedules, and relevant systems that retain records.

FINRA's report also outlines a number of possible regulatory and implementation issues for broker-dealers to consider as they explore RegTech services, including supervisory control systems, outsourcing structure and vendor management, customer data privacy, security risks and others. While the use of RegTech poses potential new challenges and most financial institutions have not yet subscribed to RegTech solutions, the financial services industry welcomes FINRA's active participation in developing a roadmap for innovation in the RegTech

space. The regulator's engagement with member firms, vendors, and the public are already leading to collaborative, impactful guidance and the evolution of new technologies to solve compliance problems.

Payments Everywhere

The payment industry has been, and will continue to be, one of the most dynamic areas of innovation in the financial services industry. As the infrastructure of payments continues to evolve, innovation will move the payments industry from a series of specific products to part of everything consumers do. Differentiation will be driven by data, technology and delivery, and changing the dynamics of how and where people pay and receive payments. Payment innovation trends will occur in conjunction with the Internet of Things (IoT), point of sale (POS), mobile wallets, cryptocurrencies, and blockchain. The impact of this innovation will be a decrease in transaction fees and an increase in the importance of differentiated user experience, and the application of vast amounts of payment data to best serve consumers in the future.

Cloud Computing

As mentioned earlier in this paper, the expansion of cloud computing is related to third-party risk, one of the top three operational risks for financial institutions today, and one that RIM professionals must closely monitor because of the potential implications on regulatory record storage. Little, if anything, can stop the evolution and growth of the cloud business. With hybrid clouds shaping up to be the most common type of cloud arrangement, the leaderboard for IaaS cloud services will likely remain unchanged: Amazon Web Services (AWS) leads, followed by Microsoft Azure, followed by Google Cloud. It seems unlikely that any other major cloud providers are going to take a substantial market share from the top three cloud providers. According to the CMSWire publication, as of June 2018 the major cloud competitors stood as follows:

1. Amazon – 62% of the market (down from 68% a year earlier)
2. Azure jumped to 20% (from 16% a year earlier)
3. Google Cloud increased to 12% (from 10% a year earlier).[24]

Experts believe that in the next five years no one company will dominate the cloud space because cloud computing will become mostly a commodity where firms pick the cheapest option. Even today the cloud providers offer almost the same services, and users are picking one vendor over the other based on their previous experience and on incentives those vendors give. For many financial services firms it does not really matter who the leader in the cloud space is, as most firms will work with multiple cloud providers in order to not rely too much on any one vendor. Refer to Section 4.3 Outsourcing (Third-party) Risk for information on how cloud computing impacts RIM.

Artificial Intelligence and Machine Learning

In the last two years AI and ML became mainstream topics in financial services firms. Complex algorithms exist today that use natural language processing (NLP) to understand written or spoken customer requests and deliver financial advice based on pre-programmed investment strategies. Algorithms have also transformed the speed and volume of trading in capital markets. Investors use algorithms to make decisions about when and where to trade and, in some cases, what and how much to trade. Algorithms are able to adapt and improve their decisions as they absorb increasing amounts of data about the outcomes of trades. NLP technologies enable computers to “read” news and other digital information sources to further evolve investment strategies and initiate trades in response.

While the rapid pace of financial industry innovation continues, traditional financial firms and regulators are just beginning to explore how ML technologies can be leveraged to achieve regulatory compliance more effectively. As such, some firms started to use ML to undertake and improve traditional control testing activities. Others are employing AI to enhance the scope and effectiveness of monitoring and surveillance tools that uncover fraud, market abuse, and money laundering.

Following are three domains in which ML solutions are relatively advanced and can be applied in a number of different ways to improve employee productivity, accelerate manual or inefficient processes, and even mitigate risk:

1) Image and video: object detection, content moderation, optical character recognition, handwriting analysis, barcode recognition, and motion detection;

2) Audio (speech): transcriptions, keyword extraction, profanity filtering, speaker recognition, emotion analysis, and demographic analysis;
3) Text: entity recognition, topic and concept recognition, sentiment and tone analysis, translation, and language detection.

To get the most out of ML technology, firms must identify use cases that can benefit from the available tools. While AI and ML technologies are still evolving, it is clear that these technologies will continue to transform the way firms operate and manage content in the next five years and beyond. Content will be automatically surfaced when it is needed, and people will be able to ask questions of their data instead of just reading it. Content will be auto-created, auto-edited, auto-quarantined, and more. Like the case with many new technologies, privacy concerns related to AI and ML will need to be addressed.

Big Data and Analytics

There has been a lot of attention paid to big data and data analytics. Financial services have been investing in big data infrastructure for several years now, and collecting big data in ever-expanding data lakes and data centers. However, the one thing they have not been doing with big data is actually using it to further their business. Analysts estimate that only 10% of data collected is being analyzed, which leaves 90% of data unexamined and unleveraged. Some of the reasons firms are not leveraging their big data anywhere near its full potential are the disconnect between IT and Business Intelligence (BI) stakeholders, outdated storage infrastructure of data warehouses, the right data is not being collected, data collection is not standardized, data is not accurate, and ineffective and incoherent data analytics strategies.

A typical financial services firm has a huge collection of siloed customer data from sources such as call center conversations, bank websites, application access logs, social media, geolocation data, and more. Using data comprehensively will be a key to success in the future enabling firms to better understand the critical insights in the aggregated data sets to improve productivity and brand viability. The user experience is a major differentiator in the financial services industry and firms can no longer afford to hide in all that unused big data to stay competitive. They will need to start realizing the potential big data presents to grow customer satisfaction, raise brand loyalty, and tailor customer products to both market and individual customer needs.

One major issue big data presents to RIM, Risk, and Information Security and Privacy professionals is that many organizations keep accumulating big data but never dispose of any of it because they do not know what information they will possibly need in the future. The problem is that maintaining huge data lakes means the firms are maintaining a gold mine for hackers. This leads to a dilemma: what is more valuable? Protecting information that might be useful later, or reducing a risk surface that otherwise would grow exponentially? Firms must use good information governance to balance the desire to keep everything versus the need to reduce risk.

Blockchain

Blockchain is a breakthrough technology that is sparking innovation and research and development (R&D) across multiple industries. Blocks in the blockchain represent valid transactions that are hashed, encoded, and chained together in chronological order to form a ledger (database). Access to the blockchain allows access to the entire ledger and the history associated with the blockchain. Blockchain is a decentralized technology as there is no central location for information, and the network can be comprised of thousands/millions of users. When confirmed by a consensus of the network, the information becomes a permanent digital record on the blockchain. This allows the blockchain to serve as a verification and authorization tool, and it can create a trusted transaction of records.

Since the arrival of blockchain in 2009, financial services firms have historically led blockchain R&D and investment with projects beginning in 2015 or earlier. The usage of blockchain in the financial sector today has far exceeded its initial cryptocurrency, also known as virtual coin, digital asset, or virtual currency applications. Figure 6 illustrates some examples of potential blockchain usage in financial services.

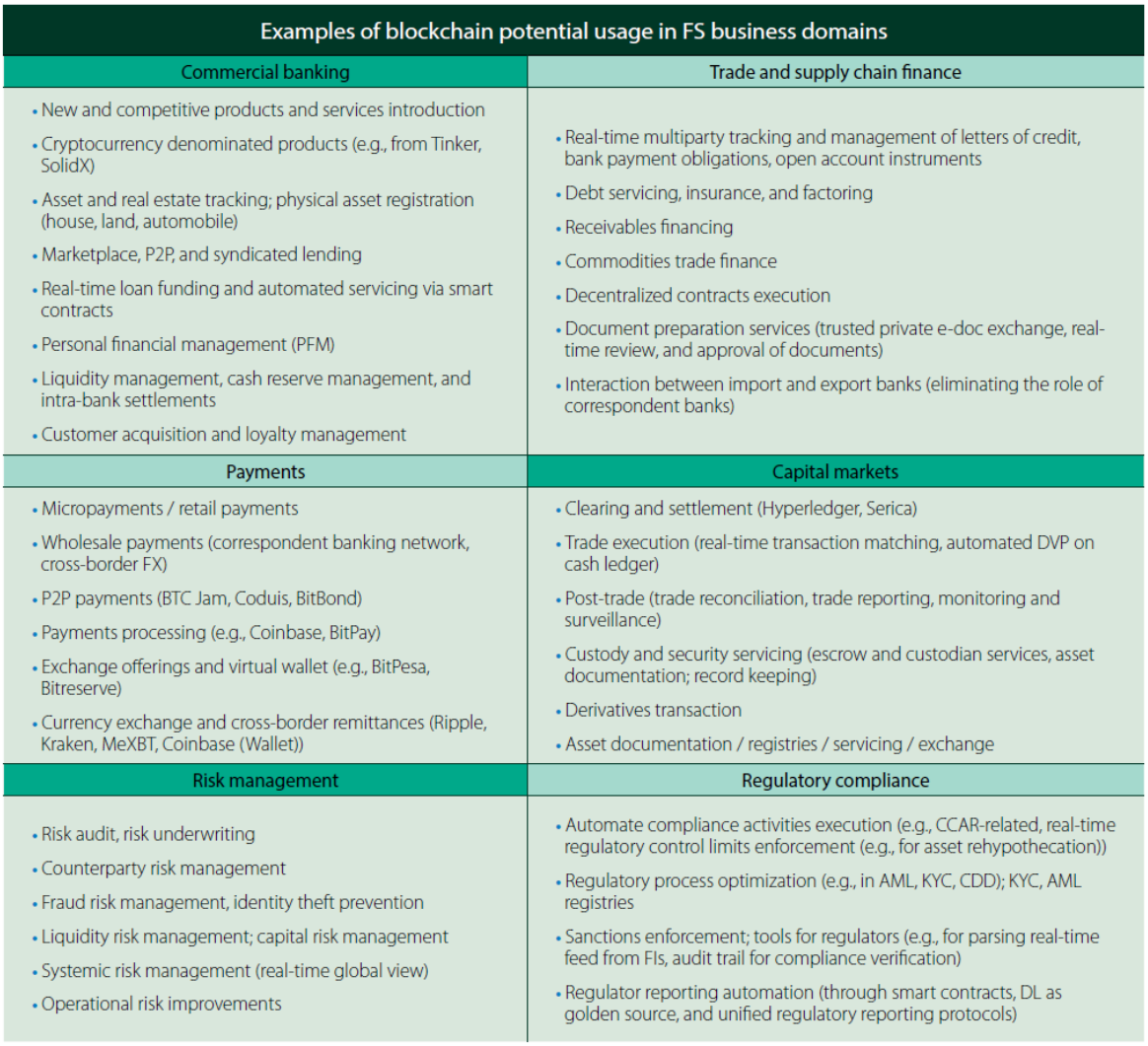

Figure 6 – Examples of Blockchain Potential Usage in Financial Services **Source: Infosys, 2018**

Proof-of-concepts continue to constitute the largest types of enterprise R&D activity. Santander, RBS, JP Morgan, Citibank, BNY Melon, UBS, Deutsche Bank, Barclays, American Express, Visa, MasterCard, and Goldman Sachs, among others, are conducting multiple blockchain-related efforts and have internal working groups or dedicated professionals focusing on blockchain technology.

For financial institutions, blockchain promises huge savings in infrastructure costs. It can remove the need for intermediaries in the digital transfer of financial assets, reducing the role of central counterparties. It can also help improve the level of trust, accuracy, and resilience in the

financial ecosystem. Due in part to regulations, financial institutions are testing blockchain in a measured and conservative manner. Firms have gravitated to blockchain consortia as they pursue R&D. Many banks are in the R3CEV (or R3) consortium, which is dedicated to banking. Many are also in the Hyperledger consortium and the Ethereum Enterprise Alliance (EEA), as well as others.

The specifics of R&D efforts by financial firms are not always publicly known, but following are some examples of how blockchain technology is being explored by various firms:

- JP Morgan, a member of the EEA and Hyperledger consortia, has an internal blockchain team, along with its own blockchain infrastructure called Quorum, specifically designed for financial services transactions. In October 2017 the company announced the launch of an inter-bank payment platform called the Interbank Information Network.
- UBS, Deutsche Bank, BNY Melon, and Santander pioneered a blockchain-based digital token that could form the industry standard for trades clearing and settlement.
- In March 2017, MasterCard applied for a patent for the blockchain-based storage of payment histories between vendors and customers.
- In April 2017, American Express applied for a patent for a new customer rewards program that uses blockchain for recordkeeping and cryptocurrency for rewards points.
- In November 2018, Visa unveiled a pilot of its blockchain-based business-to-business payments service called B2B Connect.

In recent years, various blockchain technology platforms have been and are being developed. Over 300 technology startups, mostly in the U.K. and the U.S., have been working on enabling blockchain for the financial services space. R3, IBM, and Chain are currently the dominant players in the global blockchain technology market. Regulators globally, including CFTC, SEC, NYDFS, and FRB in the U.S., have begun focusing on blockchain's adoption by the financial sector. Regulators recognize that extensive international cooperation would be required to achieving a balanced regulatory framework for blockchain applications.

Firms face several challenges as they consider the adoption of blockchain technology. Most importantly, many fundamental blockchain technologies are unready and untested for large-scale enterprise implementations. While blockchain allows for disintermediation of central

counterparties from databases and processes, they have slower transaction processing times. Another area of concern is privacy and security. By default, chains of transactions on blockchain are visible to all of the network participants and could be traced publicly. Blockchain systems also lack security which is evidenced by recent security breaches in the news, as well as many breaches that have been kept secret from the public.

Regulatory risk is one of the most important risks financial services firms must manage, and blockchain technology today presents a number of regulatory compliance concerns. There is a lack of regulatory clarity on blockchain, starting with the definition of the product or asset. Regulators are still analyzing cryptocurrencies to determine what purpose they serve, how they are marketed and to whom, and how they perform over time. Once the use is better understood, regulators can then determine whether they can apply the same regulations governing similar products and activities, where possible, or if there will be a need to define a new class of asset or service. As such, regulators determined that the initial coin offering (ICO) meets the requirements of an investment contract, which means that they have to be registered with, and regulated by, the appropriate financial regulators. Further, if the ICO is considered a security, then SEC and FINRA rules apply. Alternatively, if the ICO is considered a commodity, then CFTC rules apply. The SEC instituted 20 enforcement actions relating to cryptocurrencies in 2018. Sanctions have included 1) monetary penalties, 2) registration and compliance with securities laws, and 3) novel requirements to return or destroy digital assets. Regulators are also concerned that existing blockchain setup may not be fully compliant with privacy regulatory mandates, such as the right to request deletion of data under GDPR, CCPA, and other privacy laws.

There is a chance that the blockchain community does not resolve these challenges and the technology does not live up to its grand expectations. However, if the experts leading the blockchain field address critical technical, privacy, security, and regulatory challenges, and the financial industry begins to see production implementations of enterprise-level blockchain applications, the promise of blockchain may be realized in the years to come. RIM professionals need to follow the developments in the blockchain field to be prepared to respond to any impacts related to records retention once this innovative technology becomes more mainstream, understood, and production-ready.

Impact of New Technologies

The investment by financial institutions in some of the new technologies described in this Section is still limited due to technology immaturity, cost, the difficulty of working around cumbersome legacy systems, and uncertainty over how regulators will respond. However, the speed and the rate of change brought about by new technologies is forcing RIM, Risk, and Compliance professionals, as well as regulators, to look into these new technologies and understand their impacts. RIM must be closely aligned with other Risk and Compliance functions and proactively monitor the industry trends and developments to be able to ensure continued compliance with regulations and internal RIM policies.

7. RIM Placement within the Organization

There is no one standard alignment of RIM within financial services organizations. Often, the placement of RIM can be explained by the history of the RIM function within each firm. Some organizations place RIM under Administrative Services because in most firms, RIM started as management of paper records and over the years expanded into electronic records. In other firms, RIM is aligned under Legal or Compliance due to the fact that the business case for RIM was built as a result of firms suffering legal issues caused by lacking or inefficient RIM practices. In some firms, RIM is placed in IT because IT is the custodian of all electronic systems and share many of the same goals as RIM, including proper record classification and metadata management, improved data governance, enforcement of retention policies, avoidance of over-retention, containment of IT infrastructure and maintenance costs, and an effective e-discovery process, to name a few. In recent years, some organizations have placed RIM under Information Security or Data Privacy functions because of the information security and privacy risk that unmanaged records and information create for the firms.

While the key executive sponsor(s) advocating for RIM may vary based on the placement of RIM within the financial services organizations, the RIM mandate remains the same. Some may argue that certain alignments have a better chance at getting the required funding for RIM initiatives than others. As such, due to the fact that cybersecurity risk is the number one operational risk for financial services organizations, and the one that is expected to increase in importance the most over the next several years, the Security functions today typically are able to secure very big budgets, unlike other areas of the firms. That being said, regardless of the placement of RIM within the organization, the formula for success of an information management program remains the same – executive support, cross-functional collaboration, and the consistent enterprise-wide implementation of RIM policies, standards, and best practices all lead to a sustainable and legally defensible RIM program that reduces information risk and increases information value.

8. Future Industry Outlook and RIM

In order to compete and grow when margins are shrinking, competition is fierce, regulations are changing, and technology has an increasing impact, financial institutions must place innovation as a top priority. Organizational cultures must shift to support innovations, which will impact not only increasingly outdated business models, but perhaps entire organizations that fail to recognize the significance of innovations in maintaining their competitive position and staying in business. Firms will also put a stronger focus on improving the customer experience to be able to innovate in ways that prioritize the most effective mix of capabilities, processes, and people.

In 2019 and beyond, firms will place a big emphasis on digitizing core business processes to be better prepared for the future. The importance of innovation and developing new solutions that take advantage of data, advanced analytics, digital technologies, and new delivery platforms is at its highest. As part of these mega-trends, firms will also experiment with new mobile applications and voice-enabled tools to enhance delivery and contextual personalization. As technologies continue to evolve, the financial services sector will continue to increase its investments in innovation and digital enhancements.

The job of RIM professionals in this rapidly changing business environment is to become a “profit protection center” for the business. RIM processes must be cognizant, agile, and adaptable to the constantly changing regulations, non-regulatory drivers, risks, and innovations to support the objectives of growing and transforming the business, while making sure it is done in a compliant way. In order for RIM professionals to do the job effectively, executive management needs to recognize the importance of sound information management and allocate resources to acquire, train, and provide on-going professional development for RIM staff, fund RIM initiatives, and ensure RIM is at the table with other stakeholders making information management decisions. RIM professionals should stay abreast of financial services industry trends and RIM best practices, including participating in industry think tanks and conferences, leveraging educational resources provided by industry associations, such as ARMA International and SIFMA, and joining peer groups. As with any industry, the success of RIM in financial services relies on collaboration of many stakeholders across the organization to bring the

common vision of sound, legally-defensible information governance to the forefront where information is raised to the same level as other key organizational assets.

Appendix 1

Credit Suisse Pleads Guilty, Pays $2.6 Billion To Settle U.S. Tax Evasion Charges

"Credit Suisse failed to retain key documents, allowed evidence to be lost or destroyed, and conducted a shamefully inadequate internal inquiry." said Attorney General Eric Holder

FINRA Fines 12 Firms a Total of $14.4 Million for Failing to Protect Records From Alteration

"…Federal securities laws and FINRA rules require that business-related electronic records be kept in WORM format to prevent alteration. The SEC has stated that these requirements are an essential part of the investor protection function because a firm's books and records are the "**primary means of monitoring compliance with applicable securities laws**…"

Citigroup agrees to pay $7m penalty

Citigroup has agreed to pay a record $7 million penalty to settle charges that it provided incomplete "blue sheet" information.

"Broker-dealers have a core responsibility to promptly provide the SEC with accurate and complete trading data for U.S. to analyze during enforcement investigations," Robert A. Cohen, co-chief of the SEC enforcement division's market abuse unit. "Citigroup did not live up to that responsibility for an inexcusably long period of time, and it must pay the largest penalty to date for blue sheet violations."

Deutsche Bank Fined $6m

The Financial Industry Regulatory Authority (FINRA) today announced it has fined Deutsche Bank Securities Inc. $6 million for failing to provide complete and accurate trade data in an automated format in a timely manner when requested by FINRA and the Securities and Exchange Commission (SEC)

DB Fined $2.5bn

for its involvement in the Libor and Euribor rate-rigging scandal.
"The bank took far too long to produce vital documents and it moved far too slowly to fix relevant systems and controls," said Georgina Philippou, acting director of enforcement and market oversight.

Morgan Stanley — $1.5 billion

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005) – $1.5 billion judgment entered against Morgan Stanley, in part, as a result of its failure to make a good-faith search for backup tapes (judgment reversed on appeal for unrelated reasons)

LPL Financial — $9 million

Financial Services company was handed the largest fine ever by FINRA for email-related violations of securities rules. FINRA said it uncovered 35 failures of the financial services company email review and retention systems from 2007 to 2013

Merrill Lynch Bank of America Corporation — $2.5 million

In re Merrill Lynch, Pierce, Fenner & Smith, Incorporated; Securities and Exchange Commission; Administrative Proceeding File No. 3-12236 – $2.5 million civil penalty for systemic failure to preserve and produce emails in violation of Section 17 of the 1934 Exchange Act requiring two-year preservation

ING — $1.2 million

Five financial services subsidiaries allegedly failed to properly configure hundreds of employee email accounts to ensure that the emails sent to and from those accounts were retained and reviewed.

Key Definitions

Artificial Intelligence - Artificial intelligence (AI) is an area of computer science that emphasizes the creation of intelligent machines (algorithms) that work and react like humans.

Big data – Big data is a massive volume of structured, semi-structured, and unstructured data that is difficult to process using traditional techniques and has the potential to be mined for information and used in machine learning projects and other advanced analytics applications. Big data is often characterized by the 3Vs: the extreme *volume* of data, the wide *variety* of data types and the *velocity* at which the data must be processed.

Blockchain - Blockchain is a distributed database existing on multiple computers at the same time. It is constantly growing as new sets of recordings, or “blocks”, are added to it. Each block contains a timestamp and a link to the previous block, so they form an actual chain. Blockchains are used for recording transactions made with cryptocurrencies and have many other applications.

Cloud computing - Cloud computing is a type of computing that relies on shared computing resources rather than having a dedicated network attached storage (NAS) hardware or server in residence. The cloud is just a metaphor for the Internet. Cloud computing is taking services ("cloud services") and moving them outside an organization's firewall.

Cryptocurrency (also known as bitcoin, virtual coin, digital asset, or virtual currency) - A cryptocurrency is a medium of exchange, such as the U.S. dollar, but is digital and uses encryption techniques to control the creation of monetary units and to verify the transfer of funds.

Data Analytics - Data analytics is a process for analyzing sets of data to guide business decisions and test scientific theories. Data scientists, professionals who work in the field of big data and data analytics, develop statistical models in order to analyze data and use different analytics to find patterns, trends, and relationships in data sets.

Data controller – Under General Data Protection Regulation (GDPR), a data controller determines the purposes and means of processing personal data.

Data lake - A data lake is a storage repository that holds a vast amount of raw data in its native format until it is needed. While a hierarchical data warehouse stores processed data for pre-defined reasons ready to be queried by business professionals, a data lake uses a flat architecture to store unprocessed data for reasons not yet defined to be used at a later date by data scientists as need arises.

Data map – In RIM, a data map is a comprehensive records inventory of an organization's paper and electronic information that includes all the relevant IT Systems and media (online & offline) and the responsible business units, data stewards, and custodians. In recent years, organizations supplement their data map with privacy related information to catalog what data is collected, how it is used, where it is stored, and how it travels throughout the organization and beyond, as well as the legal basis for processing that data

Data processor - Under General Data Protection Regulation (GDPR), a processor is responsible for processing personal data on behalf of a controller.

Data subject - Under General Data Protection Regulation (GDPR), a data subject is any person whose personal data is being collected, held, or processed.

Defensible disposition – Defensible disposition is the process of creating and retaining, through management evidence, the specifics of the disposition/destruction of records. Management evidence is the collective term used to describe a multiplicity of specific records (policies, procedures, logs, etc.) created for the purpose of documenting the lifecycle process of how records are in fact managed. Management evidence should be created and retained in accordance with established policies and a prescribed retention.

Digital-only bank - A digital-only bank provides banking facilities exclusively through digital platforms, such as mobile, tablets, and the Internet.

FinTech – Products and companies that employ newly developed digital and online technologies in the banking and financial services industries.

Golden Source - A **golden source system**, also known as a **system of record**, is a record storage system that is the authoritative source for a given record. The **golden source record** is the official, master version of a record. There can only be one golden source record.

Information Governance – Information governance as a strategic, cross-disciplinary framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable for the proper handling of information assets.

Machine Learning - Machine learning (ML) is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed.

Mobile wallet - A mobile wallet is a virtual wallet that stores payment card information on a mobile device. Mobile wallets are a convenient way for a user to make in-store payments and can be used at merchants listed with the mobile wallet service provider.

Natural Language Processing - Natural Language Processing (NLP) is a sub-field of Artificial Intelligence (AI) that is focused on enabling computers to understand and process human languages, to get computers closer to a human-level understanding of language.

Non-record – Non-record is information, regardless of format, created or received, that does not serve to evidence the organization's functions, policies, decisions, procedures, operations, or other business activities and transactions. Non-records may include, but are not limited to copies of documents maintained in more than one location, materials available from public sources, transitory documents, personal correspondence, and reference materials, which can be disposed of at the discretion of the user.

Personal information - Under General Data Protection Regulation (GDPR), personal information is any information relating to an identified or identifiable natural person, which is someone who can be directly or indirectly identified.

Record – Record is information in any format (physical or electronic) created, received, and maintained by an organization as evidence of functions, policies, decisions, procedures, operations, or other business activities and transactions or in pursuance of legal and regulatory obligations.

RegTech - RegTech is technology that helps streamline the process of regulatory compliance, reducing cost and time spent on regulatory operations.

Regulatory intelligence - Regulatory intelligence is the area of compliance that focuses on the identification and interpretation of changes to applicable rules and regulations, frequently across multiple jurisdictions, in order to update the firm's compliance operations, including retention requirements and retention schedules.

Regulatory sandbox - A regulatory sandbox is a regulatory approach, typically summarized in writing and published, that allows live, time-bound testing of innovations under a regulator's oversight.

Structured record – Structured record is based on a pre-defined data model and comprised of clearly defined data types whose pattern makes them easily searchable. Structured records usually originate in relational databases.

Three lines of defense – The three lines of defense is a risk management model where the first line of defense for risks is the business record owner; the second line is functions that oversee or specialize in risk management (Compliance, Operational Risk, etc.); and the third line is functions that provide independent assurance, above all Internal Audit.

Abbreviations

AI – artificial intelligence

AWS – Amazon Web Services

BI – business intelligence

DLT – distributed ledger technology

ESI – electronically stored information

EU – European Union

FinTech – financial technology

GSIFI – global systemically important financial institution

IaaS – infrastructure as a service

ICO – initial coin offering

IM – instant messaging

IoT – Internet of things

IT – information technology

KYC – know your customer

ML – machine learning

NLP – natural language processing

POS – point of sale

RegTech – regulatory technology

RIM – records and information management

ROT – redundant, obsolete, trivial

R&D – research and development

SaaS – software as a service

SIFI - systemically important financial institution

Regulatory References

CCPA – California Consumer Privacy Act

CFPB – Consumer Financial Protection Bureau

CFTC – Commodity Futures Trading Commission

FDIC – Federal Deposit Insurance Corporation

FCM – Futures Commission Merchant

FCRA – Fair Credit Reporting Act

FIA – Futures Industry Association

FINRA – Financial Industry Regulatory Authority

FOIA – Freedom of Information Act

FRCP – Federal Rules of Civil Procedure

FRB – Federal Reserve Board

GLBA – Gramm-Leach-Bliley Act

GDPR - General Data Protection Regulation

ISDA – International Swaps and Derivatives Association

NFA – National Futures Association

NYDFS – New York Department of Financial Services

OCC – Office of the Comptroller of the Currency

OTS – Office of Thrift Supervision

SEA – Securities and Exchange Act

SEC – Securities and Exchange Commission

SIFMA – Securities Industry and Financial Markets Association

SOX – Sarbanes-Oxley Act

SPNB – special purpose national bank

End Notes

[1] Investopedia Internet Web site, January 30, 2019, https://www.investopedia.com/terms/f/fdic.asp

[2] FINRA Internet Web site, January 30, 2019, www.finra.org/about

[3] SIFMA Internet Web site, January 30, 2019, https://www.sifma.org/about/

[4] Petition for Rulemaking to Amend Exchange Act Rule 17a-4(f), November 14, 2017, https://www.sifma.org/wp-content/uploads/2017/11/SIFMA-Submits-Rulemaking-Petition-on-SEC-Electronic-Recordkeeping-Requirements.pdf

[5] Electronic Recordkeeping by Investment Companies and Investment Advisers, Release No. IC-24991 and IA-2945, 66 Fed. Reg. 29,224, May 30, 2001

[6] Recordkeeping, 82 Fed. Reg. 24,479, at 24,480, May 30, 2017 ("CFTC Adoptive Release)

[7] GDPR is Coming: Don't Be Left in the Dark, BDO, ZL Tech, Intel Webinar, September 20, 2017

[8] Council of Information Auto-Classification, "Information Explosion" survey, November 26, 2013, http://infoautoclassification.org/survey.php

[9] Robert F. Smallwood, Chapter 1, The Onslaught of Big Data and the Information Governance Imperative, *Information Governance: Concepts, Strategies, and Best Practices*, Wiley CIO Series, 2014

[10] Patch management worries OCC, Internet Reference, June 22, 2017, https://www.risk.net/risk-management/operational-risk/5294131/patch-management-worries-occ

[11] Global Risk Management Survey, 11th Edition, https://www2.deloitte.com/content/dam/insights/us/articles/4222_Global-risk-management-survey/DI_global-risk-management-survey.pdf

[12] Top 10 Operational Risks for 2018, Internet Reference, February 22, 2018, https://www.risk.net/risk-management/5424761/top-10-operational-risks-for-2018

[13] Banks fearful as data breach missteps and GDPR looms, Internet Reference, February 22, 2018, https://www.risk.net/risk-management/5423326/top-10-op-risks-2018-data-compromise?utm_campaign=Top%2010%20oprisk%202018&utm_medium=risk.net&utm_source=article

[14] Here's How You Clean Up Network Shares, May 31, 2018, https://www.cmswire.com/information-management/heres-how-you-clean-up-network-shares/

[15] Ten Key Regulatory Challenges of 2019: Resiliency Amidst Innovation, Internet Reference, December 4, 2018, https://assets.kpmg/content/dam/kpmg/us/pdf/2018/12/ten-key-regulatory-challenges-pov-v5-web.pdf

[16] SEA Rule 17a-4(i), https://www.finra.org/sites/default/files/SEA.Rule_.17a-4.Interpretations_0_0.pdf

[17] FINRA Regulatory Guidance 18-31, September 14, 2018, http://www.finra.org/sites/default/files/notice_doc_file_ref/Regulatory-Notice-18-31.pdf

[18] PwC's 2018 Digital Banking Consumer Survey: Mobile Users Set the Agenda, Internet Reference, June 2018, https://www.pwc.com/us/en/industries/financial-services/library/digital-banking-consumer-survey.html

[19] OCC Begins Accepting National Bank Charter Applications From Financial Technology Companies, Internet Reference, July 31, 2018, https://occ.gov/news-issuances/news-releases/2018/nr-occ-2018-74.html

[20] Statement by DFS Superintendent Maria T. Vullo on Treasury's Endorsement of Regulatory Sandboxes for Fintech Companies and the OCC's Decision to Accept Fintech Charter Applications, Internet Reference, July 31, 2018, https://www.dfs.ny.gov/about/statements/st1807311.htm

[21] Technology Based Innovations for Regulatory Compliance (RegTech) in the Securities Industry, Internet Reference, September 2018, https://www.finra.org/sites/default/files/2018_RegTech_Report.pdf

[22] Cost of Compliance 2018 Report: Your Biggest Challenges Revealed, Internet Reference, https://legal.thomsonreuters.com/en/insights/articles/cost-of-compliance-2018-report-your-biggest-challenges-revealed

[23] How RegTech Closes the Gap Between Technology and Financial Services, Internet Reference, April 26, 2017, https://www.bloomberg.com/professional/blog/regtech-closes-gap-technology-financial-services/

[24] AWS vs. Google vs. Microsoft: Who Will Win the Cloud (and Does it Matter)?, Internet Reference, January 18, 2018, https://www.cmswire.com/information-management/aws-vs-google-vs-microsoft-who-will-win-the-cloud-and-does-it-matter/

About the Author:

Anna Lebedeva, IGP, CIPM, PMP, is a vice president of records and information management compliance at a global financial services firm. With more than 20 years of experience in various professional information management and technology positions in the financial services industry, her RIM accomplishments include establishing an enterprise-wide records and information management program from the ground up, developing retention schedules, and standing up a defensible legal hold process. In addition, she has in-depth knowledge of enterprise content management. Anna recently has focused on regulatory recordkeeping compliance and privacy areas. In previous years, Anna built extensive experience and skills in software development and project management.

Anna earned her Master of Science degree in software engineering from Fairfield University and her Bachelor of Science degree in finance from the University of Bridgeport. She has been active with ARMA International at the chapter and international levels and is a member of a small group of subject matter experts selected by ARMA International to participate on the IGP Certification Exam Writing Committee. Anna holds Information Governance Professional (IGP), Certified Information Privacy Manager (CIPM), and Project Management Professional (PMP) certifications, is a published author, and is a frequent speaker at professional conferences. She volunteers her time to provide IT support for the final course project for the Digital Preservation class at the Graduate School of Library and Information Studies at Queens College, City University of New York.

The Foundation is a leading organization that that facilitates research, scholarship, and education for the information management profession.

The Mission of the Foundation is to provide current and relevant resources to information management professionals allowing them to advance the profession.

The Foundation is a non-profit corporation with 501(c)3 tax exempt status in the United States.

If you wish to fund any future research projects, please contact admin@armaedfoundation.org or visit the Foundation website www.armaedfoundation.org.

Additional Foundation financial and program information can be found at:

The National Database of Non-profit Organizations
http://www.guidestar.org/organizations/31-1556655/arma-international-educational-foundation.aspx