INSTITUTE OF INTERNATIONAL FINANCE

MARCH 2017

DEPLOYING REGTECH AGAINST FINANCIAL CRIME

A REPORT OF THE IIF
REGTECH WORKING GROUP

EXECUTIVE SUMMARY

Beginning in the early 1990s, an extensive global regulatory architecture has been built to combat the use of the financial system to launder money from illicit sources (such as corruption or crime) and to finance illicit activities (such as terrorism and the proliferation of nuclear arms). The global Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) framework is based on Financial Action Task Force (FATF) recommendations and United Nations (UN) conventions, but finds its legal basis in legislation at the domestic level. It is enforced by national law enforcement agencies. There is a near-consensus that this framework suffers from two key flaws:

1. Information sharing challenges. Money laundering and international fraud typically aim to exploit regulatory and supervisory gaps by channeling funds through multiple institutions, jurisdictions and financial constructs. Therefore, information sharing is key for financial institutions (FIs) and law enforcement agencies to track and identify suspicious activities. However, information sharing is hampered by the setup of the current AML/CFT system, in which FIs can only share information between themselves on an ad-hoc, individual basis; local laws on data sharing and privacy inhibit data sharing; and poor data quality, data infrastructures and the absence of common reporting standards reduce the quality of analysis.
2. International AML/CFT regulations have not fully removed ambiguities by leaving significant room for interpretation, leading to fragmentation among jurisdictions and conflicting sets of requirements. For example, agreement on the primary offenses in AML/CFT is still lacking, and there are uncertainties as to the validity and applicability of "know-your-customer's-customer" (KYCC) obligations on banks and the possible liabilities arising from non-compliance with such requirements.

FIs play an important role in the process of identifying and reporting suspicious activities with financial intelligence units (FIUs) of national law enforcement agencies. FIs are assigned two key responsibilities. First, know-your-customer (KYC) due diligence is the identification of clients and the gathering of information on clients' activities and sources of wealth relevant to assessing a client's risk profile in relation to potential illicit activity. Second, ongoing monitoring of payments systems and client accounts is required to detect illicit transactions and other suspicious activities.

Regtech solutions hold promise to improve the ability, speed and efficiency of FIs in analyzing and sharing data for the purpose of detecting and reporting financial crime, and complying with associated regulations. More specifically, new technologies can allow for:

- More effective detection of suspicious transactions and activities through increasingly accurate detection systems and technologies for faster, more secure and more efficient data sharing;
- Reduced human error due to automation of part of the process;
- Increased security of interactions between FIs and their clients, thus reducing vulnerability to fraud;
- More efficiency at FIs as costs of compliance are brought down.

Ultimately, it is important to note that benefits of implementation of these technologies are system-wide, and certainly not limited to FIs: Authorities largely rely on FIs to gain intelligence on money laundering and illicit financial activities. Adoption of regtech can also benefit financial inclusion as it lowers barriers to access to the financial system, and mitigates incentives for financial institutions to derisk by allowing for better risk management. To attain their full potential, implementation of regtech solutions should be accompanied by effective regulatory reforms (see

below).

Several technologies are or may in the future contribute to this advancement:

1. **"Big data" technologies** including clouds, data lakes and data processing engines provide a central infrastructure allowing FIs to gather, index (make searchable), store and speedily access vast amounts of information across their organization. As they are largely agnostic about data size, structure and type, they are well equipped to handle the wide variety of data relevant to KYC/AML investigations. Such data include transactions metadata, client information on proprietary systems, information from external sources including "deep web threat intelligence," public sources and KYC utilities.
2. **Biometrics and cybersecurity** improve the ability of FIs to unambiguously determine a client or counterpart's identity, automate onboarding and remote access to FI services, and improve the security of interactions with a client.
3. **Machine learning** has led to vastly improved analytical capabilities through its ability to apply detection rules to vast volumes of data, identify complex patterns and non-linear relationships and analyze unstructured data sources. When applied to transactions and account monitoring, it can detect suspicious activity more accurately.
4. **Robotics**, the use of artificial intelligence to automate manual tasks, can manage processes related to AML/KYC investigations. Several FIs are experimenting with robotic control over the process of acting on a money laundering alert and conducting an investigation.
5. **Shared utilities and distributed ledger technology** (DLT) could in the future be applied to AML/KYC information storage and sharing among FIs and FIUs. Today, KYC/AML information is stored in FI organizational silos behind confidential information barriers, requiring the creation of centralized intermediaries to gain efficiencies across the market. Placing this information on a distributed ledger would allow FIs to share sensitive consumer data across several entities without compromising nonpublic, personal data. Ultimately, under the decentralized business model made possible by DLT, a network of interconnected computers could collectively manage a golden source of identity information under the control of the individual consumer.

The impact of these new technologies on AML/KYC/CFT compliance is summarized in figure 1.

Figure 1. Key solutions for AML/KYC compliance and their underlying technologies

Key solution areas	Underlying technologies
1. Security solutions for unambiguous identity verification and bank-client interaction	Biometrics combined with deep learning, cryptography, distributed ledger technology
2. Automated detection of suspicious behavior on payment and client systems	Machine learning, artificial intelligence
3. Big data infrastructures: data ingestion, storage, visualization and analysis	Increased computing power, improved and cheaper data storage, faster data connections, cryptography, topology, artificial intelligence (AI)
4. Automated execution of AML/KYC investigations: analysis of internal and external data sources	Robotics and AI, big data infrastructures
5. Shared utilities and centralized data repositories	Cryptography and, in the future, possibly distributed ledger technology

RECOMMENDATIONS TO FACILITATE AML/KYC REGTECH ADOPTION

The potential of these technologies to strengthen the AML/KYC framework and improve compliance is partly dependent on the closing of regulatory loopholes and promoting better data quality across the financial system. The following actions are key in promoting regtech for AML/KYC:

1. Closing gaps in the international AML/CFT framework
    a. Provide clear, universally agreed definitions and guidelines of key regulatory concepts, including what constitutes money laundering, including primary offenses, and confirm non-applicability of "KYCC".
    b. Improve quality and timeliness of feedback and response from authorities on FI reporting, to allow obliged entities to learn and improve their reporting mechanisms and detection algorithms.
    c. Improve information sharing in the AML/CFT system so data is shared more effectively within financial groups, with the authorities, and among peer banks (including on a cross-border basis), to allow a systemic view of financial flows and activities in the international financial system.
2. Improve data sharing policy and data quality – Improved data quality and data sharing would allow authorities and FIs to obtain a more accurate, granular, up-to-date and potentially systemic view of suspicious activity on financial system infrastructures. This could be attained by improving:
    a. The ability of FIs to share data with relevant actors and authorities:
        i. Find an appropriate balance between privacy and law enforcement goals in data sharing legislation. Legislation intended to protect privacy should be tailored to the context in which sensitive data would be used.
        ii. Data laws and policy should take into account the latest technological advances, as these are significantly changing the ability to share data centrally across multiple actors while minimizing any sensitive information compromised.
        iii. FATF should work to improve the effectiveness of its member states' information sharing regimes by incorporating clearer guidance on this topic in its Recommendations.
        iv. Enhance national and multilateral programs for the financial sector and government to exchange and analyze intelligence to prevent, detect and disrupt money laundering.
        v. Governments should build on the work of the FATF to institutionalize analysis of national laws and regulations potentially impeding effective information sharing and establish international norms for consistent legislation and regulation where possible.
    b. Data formats and standardization:
        i. Standardization of data formats is key to promoting data sharing by enabling integration and helping address coordination challenges posed by regulatory fragmentation.
        ii. The adoption of FATF Recommendation 16 on Payments Data Quality should be

strengthened.

iii. Unique identifiers to transactions and legal entities (such as the Legal Entity Identifier (LEI) and Unique Trade Identifier (UTI)) should be embedded in transaction messages for unambiguous identification of parties to a transaction. In the long term, AML/CFT enforcement could also benefit from a unique identifier being applied to non-financial corporate clients of FIs.

3. Standardizing translation through phonetic standards between different scripts could prevent confusion on the spelling of names.

   a. **Create a proper environment for regtech experimentation** – It is vital that FIs have appropriate supervisory room to experiment with new technologies to improve AML/KYC compliance.

   b. To mitigate the risk of experimenting with, and migrating to, new technologies, regulators could work to enable an experimenting environment in which FIs would feel comfortable sharing information about compliance challenges and experiment with the application of new technologies.

   c. Financial institutions by themselves can improve their ability to adopt regtech by first altering procurement procedures, which are typically skewed to incumbent vendors, by requiring track records and secondly preparing their IT infrastructures for the adoption of new technologies.

4. **Shared utilities should be able to carry responsibility and liability** in order for FIs to be able to rely on their information without extensive double-checks.

5. **Make regulation and supervision resilient to continuous technological innovation.** Innovations can materially change the nature of a regulatory activity and its associated risks. Regulatory frameworks should reflect that, or risk becoming obsolete or based on out-of-date assumptions.

6. **Change supervisory focus as automation alters the nature of risk in the financial sector.** Due to automation, model risk and cyber risk will likely increase notably.

INTRODUCTION

Despite considerable investment and commitment by both the public and private sectors, there seems to be a near-consensus that the existing AML and CFT system is not working effectively to stop illicit financial flows.[1] Money laundering flows around the world are estimated to be significant, and the flow of illicit funds from emerging markets is still growing. Thereby, new regulations intended to detect, penalize and stop financial crime may have had the unintended consequence of several FIs "de-risking" by retreating from high-risk markets and activities, such as correspondent banking.

As such, there is a great urgency to improve the ability of financial institutions to detect and analyze suspicious financial activities, share information related to AML/CFT enforcement among relevant actors, and streamline associated processes for quick and effective compliance and reporting. This report maps the potential of new technologies, also called "regtech" for financial crime compliance, to contribute to these goals.

The report proceeds as follows. Chapter 1 will outline the existing AML/CFT framework, based on international agreements combined with national legal frameworks and enforcement regimes. Chapter 2 observes that the efficacy of the current AML/CFT framework is limited, and given that, identifies several key flaws in the AML/CFT framework, including data sharing challenges and ambiguous AML/CFT regulations. Chapter 3 discusses how new technologies can be applied by FIs to improve compliance with AML/CFT regulations: more effective detection of suspicious transactions, increased security of client interactions, better identification of clients through the use of biometrics, automation of AML/CFT analysis, and new ways to share sensitive information securely and efficiently across organizations. Lastly, Chapter 4 provides recommendations on how regulation can improve the effectiveness of new technologies in detecting financial crime and complying with AML/CFT.

This effort is a collaboration between the IIF Regtech Working Group, consisting of 37 global financial institutions, and IIF staff.[2] The report has been based on the valuable inputs and insights of the Working Group, grounding it solidly in the practice at financial institutions of detecting and reporting financial crime, applying new technologies, and mapping the potential of new technologies.

1 For example, Juan C. Zarate and Chip Poncy, "Designing a new AML system," in: Banking Perspectives Q3 2016, vol. 4, iss. 3; Global Financial Integrity, "Illicit financial flows from developing countries: 2004-2013," December 2015; panelists on "The future of AML and de-risking" at the IIF Annual Membership Meeting, October 2016.

2 For more information on the IIF's work on regtech, fintech and related innovations, please visit www.iif.com/topics/innovation.

CHAPTER 1 – COUNTERING FINANCIAL CRIME AND COMPLYING WITH ASSOCIATED REGULATIONS

MONEY LAUNDERING, TERRORISM FINANCING AND RELATED ILLEGAL ACTIVITIES

This report focuses on several specific types of financial crime: money laundering, terrorism financing, and evasion of sanctions. Money laundering is the process by which proceeds from a criminal activity such as drug trading, corruption or human trafficking are disguised to conceal their criminal origins.[3] The proceeds typically follow a diffuse path through the financial system in which they are converted into different financial instruments, contracts or currencies, broken into different amounts, mixed with legal funds, and/or placed at different institutions in different jurisdictions. Banks are especially vulnerable to money laundering due to their central role in the payments system and the wide variety of financial products and services they offer. However, the services of insurers, securities firms, asset managers and other FIs are also (ab)used to launder money.

Terrorism financing is the financial support, in any form, of terrorism or those who encourage, plan, or engage in terrorism, while proliferation financing concerns the provision of funds or financial services for the manufacture, transfer or possession of nuclear, chemical or biological weapons and related materials.[4] They essentially apply the same techniques as money laundering to conceal the sources of, and uses for, the financing concerned.

Corruption concerns the abuse of public office for private gain, including through bribery and theft. According to the World Bank, about 1 trillion US Dollars (USD) is paid each year in bribes around the world, and the total economic loss from corruption is estimated to be many times that number.[5] Money laundering and corruption are closely related: corrupt officials may attempt to use services from financial institutions to store or launder the proceeds of corruption. The reverse is true as well: the prevalence of money laundering may lead to more corruption and crime.[6]

Evasion of financial sanctions is closely related to money laundering and terrorism/proliferation financing. As part of AML/CFT policy, jurisdictions or international organizations can sanction countries or groups engaging in money laundering or terrorism/proliferation financing by prohibiting financial transactions with them or freezing their assets. When those sanctions are evaded by individuals or firms, they can be penalized under national legal systems.

THE CURRENT AML/CFT FRAMEWORK

International agreements

Around the world, AML/CFT policies are based on a complex set of national and international regulations, standards and guidelines. The global AML/CFT framework is primarily based on the "40+9" recommendations of FATF: 40 recommendations to members on anti-money laundering, plus nine special recommendations on terrorism financing. Additional definitions and legal agreements regarding AML/CFT are provided by the UN's Vienna and Palermo Conventions.[7]

3 P.A. Schott, "Reference guide to Anti-Money Laundering and Combating the Financing of Terrorism," joint publication of the World Bank and the International Monetary Fund, Washington 2006.

4 Financial Action Task Force (FATF), "Combating proliferation financing: a status report on policy development and consultation," FATF report, February 2010.

5 World Bank, "Helping countries combat corruption: the role of the World Bank," available at www1.worldbank.org/publicsector/anticorrupt/corruptn/cor02.htm. Also, "Anti-corruption," World Bank Brief, May 10, 2016, available at www.worldbank.org/en/topic/governance/brief/anti-corruption.

6 Schott 2006, p. II-3.

7 UN Vienna Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988), and the UN Palermo Convention Against Transnational Organized Crime (2000).

These agreements and conventions have put in place a system intended to support the ability of national law enforcement authorities (or FIUs) to trace and prosecute illicit financial activities.

Legal basis in jurisdictions

The legal basis of the system is found at the national level, in law like the European Union's Fourth Anti-Money Laundering directive or Japan's Foreign Exchange Law. The United States' set of reporting and compliance requirements is arguably the most influential internationally, as it affects all FIs doing business or transacting with a US legal or natural person or through the US or (generally) in US dollars. It is enshrined in the Bank Secrecy Act, the USA PATRIOT Act, and most recently the Foreign Account Tax Compliance Act (FATCA). Other bodies of law, such as the Foreign Corrupt Practices Act also inform the context of AML/CFT efforts.

REGULATORY REQUIREMENTS FOR FINANCIAL INSTITUTIONS

The international AML/CFT framework relies heavily on FIs to gather information on illicit financial flows and activities. FIs submit Suspicious Activity Reports (SARs) to law enforcement agencies containing detailed information on suspicious transactions.[8] Based on information obtained from the financial sector and their own investigations, law enforcement agencies then decide on prosecuting individuals or groups involved in financial crime. Additionally, when countries are sanctioned, financial transactions with those countries are prohibited.

The efforts of FIs are subject to local regulations based on the FATF's risk-based approach (RBA) to AML/CFT. The RBA holds that "countries, competent authorities and FIs are expected to identify, assess and understand the money laundering/terrorism financing risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively."[9] To supplement this high-level approach, the Basel Committee on Banking Supervision (BCBS) has released an updated set of guidelines to support the national implementation of the FATF standards for banks.[10] In addition, the FATF has recently released revised guidance on due diligence for correspondent banking activities.[11] Together, these guidelines and recommendations set a standard for regulations in each jurisdiction, but are not directly applicable or legally binding.

Under AML/CFT regulations, financial institutions need to pursue two policies to gather information on illicit activities[12]: 1. KYC due diligence and 2. Ongoing monitoring (OM) of payments systems and client accounts to identify suspicious activity and transactions. In support of these policies, the BCBS and the FATF have issued additional requirements on information sharing and management within financial institutions.

KYC

Know-your-customer due diligence involves the identification of clients and the gathering of information relevant to assessing client risk profiles. Basically, a bank has to know who it is dealing with in order to be able to make an informed assessment of whether that client is (prone to) engaging in financial crime.

Regulations prescribe that a bank should have clear, systematic procedures and policies to identify and verify its customers and, where applicable, any person acting on their behalf and beneficial owner(s) of transactions, which may be different from the bank's immediate customer.

8 Juan C. Zarate and Chip Poncy, "Designing a new AML system," in: Banking Perspectives Q3 2016, vol. 4, iss. 3.
9 Financial Action Task Force (FATF), "Guidance for a risk-based approach: the banking sector," October 2014, p. 6.
10 Basel Committee on Banking Supervision (BCBS), "Sound management of risks related to money laundering and financing of terrorism," February 2016.
11 Financial Action Task Force, "Guidance on correspondent banking," October 2016.
12 BCBS, "Guidelines: Sound management of risks related to money laundering and financing of terrorism," February 2016.

The bank should identify the customer using "reliable, independent source documents, data or information." Also, a risk assessment of the customer should be performed based on factors relevant to the situation, such as "a customer's background, occupation (including a public or high-profile position), source of income and wealth, country of origin and residence (when different), products used, nature and purpose of accounts, linked accounts, business activities and other customer-oriented risk indicators," in order to determine the level of overall risk and the appropriate measures to be applied to manage those risks.[13]

Additional scrutiny is required for those clients who "are or have been entrusted with prominent public functions in a foreign country," called Politically Exposed Persons (PEPs) in FATF terminology. For these persons, FIs need to establish the source of their wealth and funds, and they need to be subject to enhanced ongoing monitoring (see below). However, as no official organization publishes a list of PEPs, finding out whether a client is a PEP is often a significant challenge.[14] Thus, FIs need to include family members and other associates in assessments of PEPs, contributing to the overall complexity of gaining appropriate information and assessing the risk profile of PEPs.

KYC is an ongoing, continuous process, and not just a procedure that is performed as a new client joins a bank. Rather, the bank should continuously gather information to build an understanding of the customer's profile and behavior (customer risk profiles). The purpose of a relationship or an occasional banking transaction, the level of assets or the size of customer transactions, and the regularity or duration of a relationship are examples of information typically collected.

Ongoing monitoring

The FATF recommends (and national legislation requires) that all banks should be required to have systems in place to monitor payment systems and client accounts on a continuous basis to identify unusual or suspicious transactions or patterns of activity. Examples are transactions that do not appear to make economic sense, that involve large cash deposits or that are not consistent with the customer's normal and expected transactions.

Information management and sharing

To support the gathering of information on financial crime, the BCBS recommends that banks record all information obtained in the context of customer due diligence and have appropriate integrated management information systems to provide business units and risk and compliance officers with timely information. In financial groups, policies and procedures should be designed to identify, monitor and mitigate group-wide risks. "Every effort should be made to ensure that the group's ability to obtain and review information in accordance with its global AML/CFT policies and procedures is not impaired as a result of modifications to local policies or procedures necessitated by local legal requirements." However, these requirements sometimes conflict with local regulations on data privacy, data usage, handling of information reported to the authorities, and other matters, which require FIs to retain information and self-standing IT systems within a subsidiary or jurisdiction.

13 Idem.
14 Schott 2006, p. VI-9.

CHAPTER 2 – CHALLENGES AND FLAWS IN THE CURRENT FRAMEWORK FOR COUNTERING FINANCIAL CRIME

In recent years, FIs have made a great effort to scale up their capacity to identify illicit financial activity. Compliance with associated regulation has proved to be quite costly. An IIF survey among large and mid-sized member FIs shows that costs related to AML/CFT make up a significant portion of total compliance costs and staff, varying from roughly a third to 80%. Compliance costs have risen significantly in the last couple of years. At the same time, some firms have faced billions in fines for failure to comply, leading to additional investments in remediation efforts as well as the need to hold more capital against operational risk.[15]

However, despite efforts by law enforcement agencies, FIs and regulators, statistics show that financial crime has far from disappeared from the international financial system. Organized crime groups, terrorist organizations and rogue states keep finding access to illegal channels of financing to fund their activities and increase their wealth. The UN has estimated that the amount of money laundered globally every year is equal to 2% to 5% of global Gross Domestic Product (GDP). That is equal to 800 billion to 2 trillion USD; a figure that actually may be increasing.[16] Global Financial Integrity, a Washington DC-based financial crime watchdog, has found that illicit outflows from developing and emerging economies have increased at 6.5% per year in the ten years before 2013. That is nearly twice the growth rate of global GDP.[17]

FIs are equally affected by the adverse consequences of financial crime. According to the World Bank, money laundering and terrorism financing may harm the soundness of a country's financial sector and the stability of individual FIs through reputational, operational, legal and concentration risks.[18] Each of these risks has specific costs, including loss of profitable business, liquidity problems through withdrawal of funds, termination of correspondent banking facilities, investigation costs and fines, asset seizures, loan losses and declines in the stock value of FIs.

In some cases, the most practical response to financial crime risk, particularly in the AML/CFT arena, may ultimately be to "de-risk" by pulling out of entire jurisdictions or business lines.[19] All international banks perform customer-by-customer risk-based analysis, but the effect may be the same: many or most customers in certain businesses or certain jurisdictions may appear to be too risky to deal with. Correspondent banking activities have been particularly affected given their cross-border nature. Correspondent banking has been defined by the Wolfsberg Group as "the provision of a current or other liability account, and related services, to another financial institution, including affiliates, used for the execution of third party payments and trade finance, as well as its own cash clearing, liquidity management and short-term borrowing or investment needs in a particular currency."[20] It allows banks to access payment services in different jurisdictions and provide cross-border payment services to their customers.[21]

In 2015, a World Bank survey found that roughly half the banking authorities and slightly more local and regional banks indicated a decline in correspondent banking relationships. For large international banks, the figures are significantly higher at 75%. This trend particularly impacts

15 Basel Committee on Banking Supervision, "Standardised Measurement Approach for operational risk," Consultative document, Basel, March 2016, p. 13.
16 United Nations Office on Drugs and Crime, "Money-laundering and globalization," https://www.unodc.org/unodc/en/money-laundering/globalization.html.
17 Global Financial Integrity, "Illicit financial flows from developing countries: 2004-2013," December 2015.
18 Schott 2006, p. II-4.
19 The term "de-risking" has become common shorthand for referring to any instances in which banks have adopted increasingly stringent financial crime-related policies to reduce their exposure to potential money laundering, terrorist financing, corruption or sanctions risk. More specifically, it relates to the strategies adopted by banks to reduce or eliminate their risk exposure. The term tends to be used particularly where multiple businesses in a given category or country are affected.
20 The Wolfsberg Group, "Wolfsberg anti-money laundering principles for correspondent banking," 2014.
21 Committee on Payments and Market Infrastructures (CPMI), "Correspondent banking," Basel, July 2016.

services like check clearing, clearing and settlement, cash-management services, international wire transfers and trade finance. In June, the International Monetary Fund (IMF) produced a staff discussion note highlighting that "pressure on CBR [Correspondent Banking Relationships] could disrupt financial services and cross-border flows, including trade finance and remittances, potentially undermining financial stability, inclusion, growth, and development goals… pressure on CBRs can become systemic in nature if unaddressed."[22]

FLAWS IN THE CURRENT SYSTEM

Why is the current system relatively ineffective at countering financial crime, costly and risky for FIs, and complex and costly for law enforcement? Challenges to information sharing in the system and the ambiguity of AML/CFT guidelines seem to be key reasons.

1. Challenges to information sharing

Money laundering and international fraud typically aim to exploit regulatory and supervisory gaps by channeling funds through multiple institutions, jurisdictions and financial constructs. Therefore, information sharing among affected FIs and law enforcement agencies is key to track and identify suspicious activities.

The effectiveness of information exchanges has become one of the major and recurring public policy questions for those involved in combating financial crime. The G7 has called for the enhancement of information exchange and cooperation to fight the financing of terrorism.[23] The FATF itself has said effective information sharing is one of the cornerstones of a well-functioning AML/CFT framework[24] and has encouraged the G20 to take action at the national and global level to address barriers to information sharing, including the review of data protection and privacy laws.[25] In the context of the ongoing global dialogue on "de-risking," the Committee on Payments and Market Infrastructures (CPMI) has acknowledged that if banks in a correspondent banking relationship cannot provide additional information on customers and specific transactions due to legal and regulatory restrictions on exchanging information, correspondent banks may have no alternative but to block or reject certain transactions. This may in some cases lead to the termination of some correspondent banking relationships.[26]

While it is important that this issue is well recognized by the international community, information sharing within and between FIs and law enforcement agencies remains particularly difficult in the current regulatory framework for several reasons.

First, the current AML/CFT system is based on a "one-on-one" information sharing model, which is complex, inconsistent and inefficient. In this system, individual FIs share information about specific instances of suspicious activity on their systems with their regulators or law enforcement agencies.

KYC in correspondent banking serves as an example of the system's flaws. Correspondent banks need to identify and understand their respondents' banking activities, including the types of customers they serve, and to ascertain if the respondents maintain additional correspondent banking relationships. This leads to a massive exchange of documents between correspondent banks and their respondent-bank customers. According to CPMI,

22 International Monetary Fund, "The withdrawal of correspondent banking relationships: a case for policy action," IMF Staff Discussion Note, June 2016.
23 G7, "Action Plan on ing the Financing of Terrorism," May 21, 2016.
24 FATF, "Consolidated FATF Standards on Information Sharing," June 2016, p. 5.
25 FATF, "Report to G20 on Beneficial Ownership," September 2016, p. 6.
26 CPMI, Correspondent Banking, July 2016, pp. 27-28.

the 7,000 banks that use the SWIFT network for correspondent banking have more than 1 million individual relationships, so the number of documents exchanged is presumably much higher. This typically means that the same or very similar information needs to be sent to all correspondents, making the process "complex, costly, time-consuming and labor-intensive."[27]

As a result, the construction of the AML/CFT system, in which "each institution's visibility into illicit activity ends with its touch points with [its own] customers and transactions,"[28] is poorly suited to the nature of ML/TF activities, which typically use a complex network of financial instruments and deposit accounts at different institutions and jurisdictions.[29] Authorities therefore have a hard time obtaining a systemic view of vulnerabilities across institutions on a real-time basis. Indeed, at a recent IIF event, former FBI deputy director Sean Joyce said that "the one-on-one model of information sharing is never going to be a successful model". However, the legal and technical infrastructure for sharing information centrally in the system is currently largely lacking, especially across borders.

Second, laws on data sharing, localization and privacy inhibit data sharing within the same banking group, especially if the group operates in multiple jurisdictions.[30] It is therefore complex, if not impossible, for FIs to obtain a group-wide view of illegal financial activities, even though FATF and BCBS recommend that "policies and procedures [in financial groups] should be designed to identify, monitor and mitigate group-wide risks… A bank should have robust information-sharing among the head office and all of its branches and subsidiaries." Jurisdictional rules often prohibit the sharing of local customer information with a bank's foreign operations to ensure that sensitive and private information of citizens is treated appropriately.[31]

In order to assess the extent of the challenges present for this type of information exchange, the Institute of International Finance, following consultation with the FATF, undertook a survey of its member institutions with the specific aim of identifying legal and regulatory impediments where they exist and developing a cross-jurisdictional evidence base on obstacles to the availability of financial crime related information. The survey elicited responses from 28 individual financial institutions covering information concerning 92 countries across Europe, North America, Asia, Africa and the Middle East. The findings, which represent feedback from banks in all the major financial centers of the world, is a strong indicator of views from across the global financial system. It shows that banks definitively see barriers to information exchange as an impediment to effective financial crime risk management in the enterprise-wide context; among financial institutions not part of the same financial group; and between governments and the private sector.[32] Please see chapter 4 for a more in-depth discussion of regulatory barriers.

Third, the information used to detect AML/CFT activities is often of a low quality. Many information items lack standardization, and much of the information that is available is unstructured or incomplete. As a result, the processing and analysis of information is manual

27 CPMI, July 2016, p. 19.
28 Zarate and Poncy 2016.
29 For an example of how money laundering is conducted, see Institute of International Finance, "Re: Facilitating effective sharing of AML/CFT information," Letter to FATF, Washington DC, May 25, 2016.
30 Institute of International Finance, "Re: Facilitating effective sharing of AML/CFT information," Letter to FATF, Washington DC, May 25, 2016.
31 The IIF has called on the FATF to (1) update the FATF Recommendations to enable more effective information sharing in the enterprise-wide context, among financial institutions not part of the same group, and between governments and the private sector; and (2) analyze among its members the jurisdictional legal impediments to information sharing. For more information, see IIF, "Re: facilitating effective sharing of AML/CFT information," Regulatory comment letter to FATF, May 25, 2016. Available at www.iif.com/publication/regulatory-comment-letter/iif-submits-letter-effective-information-sharing-amlcft
32 IIF, Financial Crime Information Sharing Survey Report, February 2017

in character, capacity demanding, and slow. Key examples include:

- FIs monitor payment systems on an ongoing basis to detect suspicious (patterns of) transactions. However, the international payments infrastructure is made up of different payment systems which attach different metadata to each transaction, inhibiting automated analysis of the metadata. For example, some systems use MT 202 COV messaging, while others rely on MT 103.[33] Additionally, transaction metadata is often incomplete and unstructured.
- Formats for filing Suspicious Activity Reports differ by jurisdiction.
- Several providers have developed or are developing KYC utilities, with the aim of storing customer due diligence information in a single repository. Centrally storing KYC information has obvious benefits in terms of efficiency and effectiveness. However, there is no standardized set of information that should be included in KYC utilities, and they may not collect all the information that a bank needs for a risk assessment.[34] Furthermore, data privacy, processing, and localization rules inhibit cross-border use of information in utilities, and may prevent banks from submitting relevant information to utilities. Utilities are working on solutions to these problems, such as anonymization of records, but legal and regulatory complexities may block comprehensive solutions.

Fourth, FIs' legacy IT systems sometimes inhibit them from gaining a group-wide view of customer activities in an efficient, effective way. Due to silo'ing of information, use of incompatible data formats or lack of data standardization, it may be hard to retrieve and aggregate information from different sources, even where doing so would be legally permissible and customers have agreed to share their data. As a result, a KYC compliance officer may find it hard to find out if, for example, a politically exposed person is accessing his bank's services in different jurisdictions or subsidiaries.[35]

2. International AML/CFT regulations promote ambiguity

Regulations on AML, CFT and KYC leave significant room for interpretation, leading to fragmentation among jurisdictions, overlapping different bodies of requirements, and regulatory ambiguity in several key areas. Most importantly, a universal definition of money laundering, primary offenses, and criteria on how to identify it, are still lacking. Combined with what is widely perceived as a "zero-tolerance" attitude from regulators on compliance, this ambiguity is leading FIs to over-report any potentially suspicious activities.

Additionally, the FATF and national guidance on KYC have been ambiguous on whether correspondent banks need to apply KYCC. When a correspondent bank that has done due diligence on its respondent's AML-CFT policies and procedures can nonetheless be held responsible for payments by or to the respondent's customers who turn out to be money launderers or sanctions-violators or terrorists, the cost and complexity of transaction monitoring are obviously compounded. At the same time, recent guidance published by the FATF says that "there is no expectation, intention or requirement for the correspondent institution to conduct customer due diligence on its respondent institution' customers."[36] This was intended to help the industry get beyond the perception from prior documents that KYCC may be required in some cases. Whether this new guidance will sufficiently

33 MT202 Cov and MT103 are message formats used in SWIFT systems, allowing for different ways of sending funds through intermediary institutions to a final one.
34 CPMI, July 2016, pp. 19-21.
35 Issues with FI's IT systems are further discussed below.
36 Financial Action Task Force, "Correspondent banking services," FATF Guidance, Paris, October 2016.

alleviate the problem of KYCC-based costs and burdens remains to be seen, as it will depend upon how the new guidance is implemented locally, and ultimately upon whether law enforcement agencies respect it or whether they nonetheless bring actions against banks on compliance issues in KYCC situations.

3. IT systems at financial institutions are sometimes outdated

Apart from regulatory ambiguity and obstacles to information sharing, legacy systems at some FIs may contribute to the difficulty in obtaining an up-to-date, group-wide view of suspicious activity. Legacy systems typically refer to a firm's backbone IT infrastructures – the platforms and operation systems on which many applications run. These systems may suffer from being outdated and complex or contain disconnected silos of information and duplicative processes.

Organic growth of systems has made holistic change complicated and expensive. As banks and the technology available to them have evolved over the past 20 to 30 years, multiple layers of technology platforms have been built on top of each other to facilitate changes and new requirements. Being at the heart of established FI operations, these systems are business critical, dependent upon other elements of a bank's IT infrastructure and are often running 24 hours a day. That makes it complex and expensive to add or remove elements to the core platforms.

Furthermore, mergers and acquisitions of FIs can lead to suboptimal systems. With a standard or template for the infrastructure of FIs lacking, it is a challenge to integrate systems as one institution merges with or acquires another. In many mergers and acquisitions, FIs will forego fully integrating newly acquired operations onto their existing platforms because of competing demands on time and resources.[37]

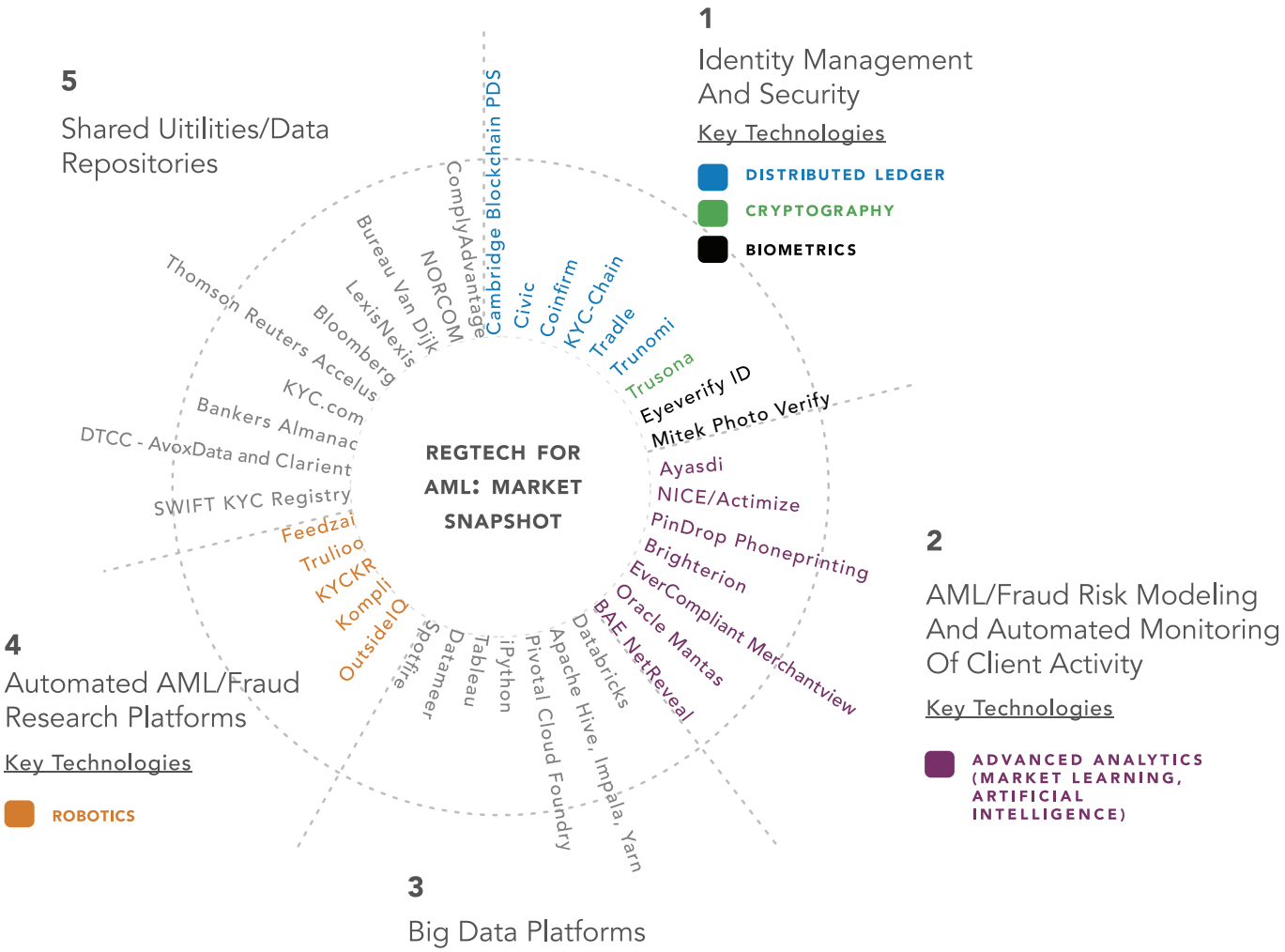
Banks are making large investments in risk data aggregation for a number of regulatory and business reasons, including pursuant to the BCBS recommendations on Risk Data Aggregation ("Basel 239"). However, it will take some time for these efforts to be fully implemented. Removing legal and regulatory inconsistencies and impediments would greatly assist and speed up the process.

37 Intellect, "Biting the bullet – why now is the time to rebuild the foundations of the financial system. The urgent case for infrastructure renewal," August 2012.

CHAPTER 3 – A ROLE FOR TRANSFORMATIVE TECHNOLOGIES

As has been discussed, the current AML/CFT system is suffering from serious deficiencies. It is clear that several of the major flaws in the current system can only be solved through updated regulation, for example with regard to information sharing. However, applying transformative technology has several key benefits in the AML/CFT/financial crime space:

- More effective detection of suspicious activity and fraud through increasingly accurate detection systems and technologies for faster and better data sharing;
- Reducing human error through automation;
- Increasing security of interactions between FIs and clients;
- Significantly bringing down costs of compliance;
- Promoting financial inclusion by lowering barriers to access to the financial system for potential customers, while allowing for a better management of risks for FIs.



This chapter further discusses six key roles which new technology can play in countering financial crime and complying with associated regulations.

1. "Big data" infrastructure: unlocking information across the organization

"Big data" technologies including clouds, data lakes, and data processing engines allow for the efficient and effective storing, accessing, sharing, processing, structuring and mining of information. These systems constitute a transformative improvement to previous data infrastructures: due to increases in computing power, they can process and store much larger amounts of data. And while traditional systems have mostly been designed to work with high-quality structured data, current systems are able to gather, index and store all kinds of data, whether structured and unstructured, without requiring strict rules as would be required of data entering an enterprise data warehouse. Unstructured data refers to data without the well-defined and consistently applied schemas, templates or constraints on data types, storage formats, and allowable values that facilitate automated analysis.[38] Examples are written text, spoken word, and also payment systems metadata.

Figure 2: Big data infrastructures: Several key underlying innovations	
Increased computing power	Improved analysis of and access to large data sets
Improved data storage	Ability to store large amounts of data at low cost
Faster data connections	Ability to access data remotely, while storing centrally in an organization; ability to store and analyze data in real-time
Cryptography	Making centrally stored data available securely to large groups of users by personalizing access per user (such as cell level security)
Topology	Ability to summarize and make searchable all kinds of data, unstructured and incomplete
Statistics, artificial intelligence	More accurate analysis of a wide variety of data sources

These systems are able to index and store such unstructured, noisy data by making use of techniques including topological data analysis (TDA), a subfield of mathematics. TDA applies the central question of topology – how to describe and summarize an object across different transformations – to the storing of data which are unstructured, varying in type, and often incomplete. It manages such data by analyzing them in a manner that is insensitive to the particular metric, summarizes the data, and is robust to noise.

"Big data" infrastructures typically consist of four components:

- A data ingestion engine such as Flume, Kafka or Akka, that processes and indexes the data, and extracts key information to archive the data as it is stored, making use of topological data analysis.
- A central data lake or cloud, on which data is stored and is made accessible. Clouds can be both public (such as the Amazon and Google clouds) and private, operating only within the firm.
- A workload management environment, allowing the infrastructure to manage different tasks and requests, like YARN, Storm or Kubernetes.
- Engines for data processing and mining, such as Apache Spark.

38 Institute of International Finance, "Regtech in financial services: technology solutions for compliance and reporting," March 2016. Available at www.iif.com/publication/research-note/regtech-financial-services-solutions-compliance-and-reporting

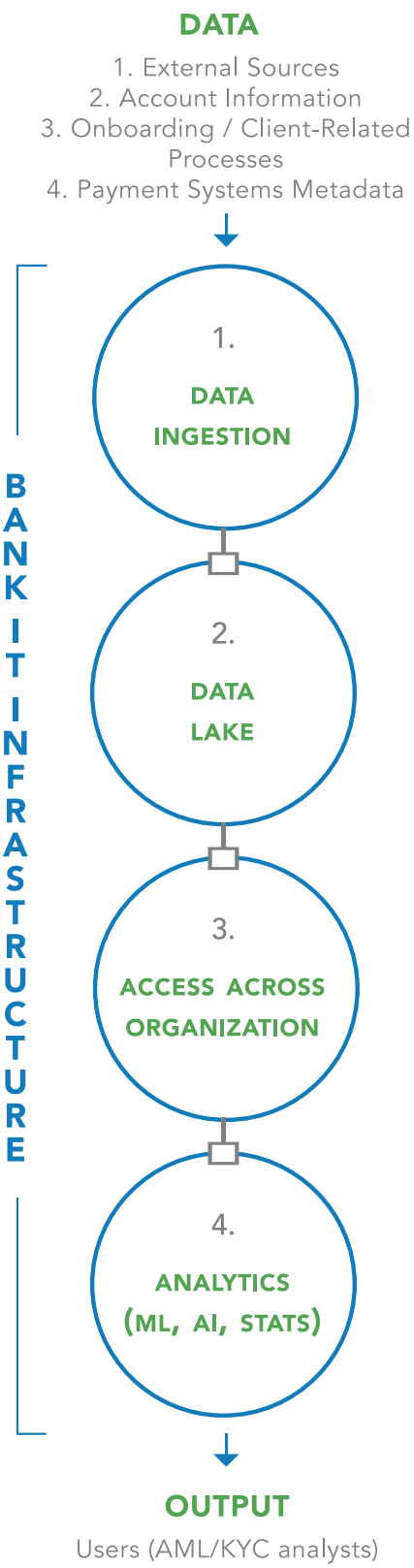
Applying big data technologies to AML/CFT

In AML/CFT compliance and the countering of financial crime, these systems can serve several purposes. First, and most importantly, these new data technologies can provide the infrastructure on which other applications can run, thereby providing an answer to some of the banks' challenges in implementing new, innovative applications on their legacy IT systems. FIs could set up a "two-speed IT architecture" consisting of a decoupled reliable back-end (the legacy systems) and a flexible, agile front-end consisting of the new "big data" infrastructure. Such a system could ingest data from all kinds of sources, with other applications tapping into them, including customer-facing onboarding and biometric identification systems and machine learning analytics. Several major banks have set up new data infrastructures in parallel to their existing, legacy systems.

In AML/CFT, these systems can be particularly useful. To investigate fraud and money laundering on their platforms, analysts at FIs access many different sources of information in many different formats: client information on the institution's own systems (address, name, gender, age, services used, deposit, credit card and other account information), metadata churned out by payment systems, public records, recordings from phone calls, open sources including social media and internet, KYC utilities, etc. Because big data infrastructures are largely agnostic about data size and structure, they provide an efficient way to access and store all these types of information.

Applying such an infrastructure across a financial group would allow FIs to access information across the group in a quick and easy way. According to Intellect, "as a general rule of thumb, the more accurate, comprehensive and readily available the data is on a bank's customers and transactions, the more likely it will be to spot fraud at an earlier stage." However, it should be noted that the creation of such efficient, cross-group data structures is not only a technical matter, as data sharing faces significant regulatory barriers (see chapter 4).

Second, through new ingestion technologies, these systems can access, index and open up both larger and new sources of information that were previously too large or too difficult to include in analysis. They also can do so in real time. In terms of data size, this means that FIs can now conduct an analysis of all their transactions, customers or other



data, rather than just a sample as was previously often the case. An example of a new information source now included in automated analysis is web crawlers scanning the internet and delivering their data to big data infrastructures. This "deep web threat intelligence" allows FIs to perform background checks on counterparties and clients through open sources.

2. Machine learning: more accurate and powerful data analysis

Advances in computing power, paired with improvements in econometrics and statistics, have led to the development of a range of sophisticated analytical tools under the heading of "machine learning". Machine learning is the subfield of computer science that "gives computers the ability to learn without being explicitly programmed". It can be applied to analyze data sets of all sorts, and is able to improve its accuracy as more data is analyzed. This method provides several benefits.

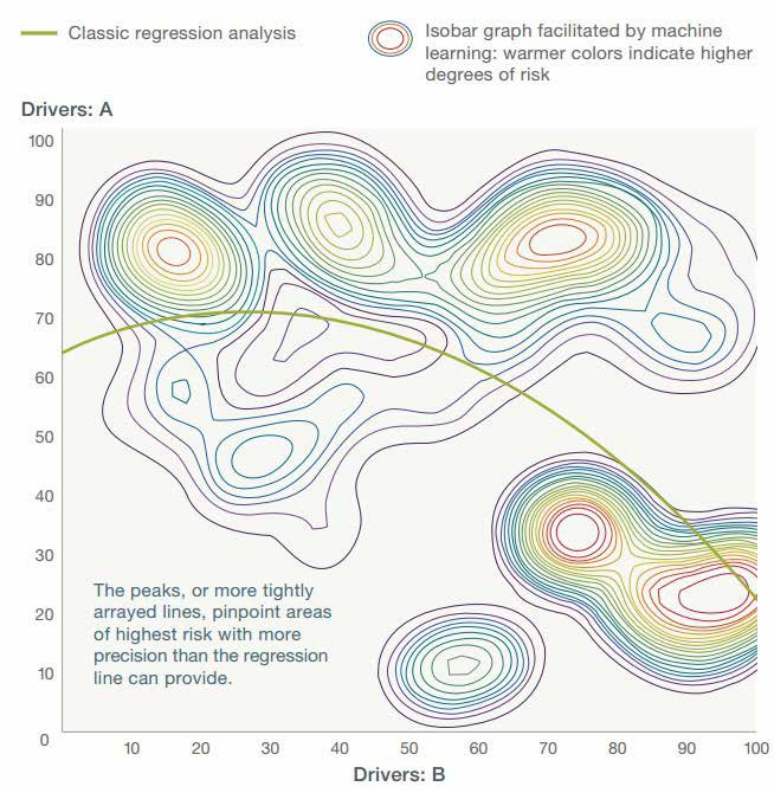


Figure 3: Example of analysis of relations in a data set through a classic regression analysis and machine learning analysis. Machine learning technology is able to describe data relationships in greater detail and with more dimensions.
Source: Dorian Pyle and Cristina San Jose, "An executive's guide to machine learning," in McKinsey, "FinTechnicolor: the new picture in finance," June 2016.

First, improved analytical capabilities. Machine learning is able to find relationships in datasets with much greater accuracy and in more dimensions than previous statistical methods, including regression analysis (see figure 3). It is able to identify non-linear relationships and other interactions in the data that other statistical methods have been unable to detect. FIs are increasingly applying this technology to develop more accurate risk models. One area in which machine learning has been applied for quite some time and with significant success is credit card fraud. In money laundering, it would under the right circumstances be able to find complex patterns of suspicious activity.

Machine learning's improved analytics could constitute a major improvement in the ongoing monitoring of payment systems by analyzing transactions metadata on payment systems to detect (patterns of) suspicious transactions. Thus far, payment systems have been mostly monitored by rules-based detection systems; however, as these systems are able to focus only on individual transactions, they are unable to detect complex patterns of transactions or obtain a holistic view of transaction behavior on payment infrastructures. Rules-based systems also produce many false positives, requiring human evaluation to determine whether an alert actually qualifies as suspicious activity. In comparison, machine learning-

based systems can bring down the number of false positives significantly.[39]

When embedded in a big data infrastructure providing real-time data ingestion and processing, machine learning payment processing capabilities could in the future monitor all transactions in an FI at network speed. Such an application could alter the character of AML/KYC compliance from monitoring to prevention: monitoring transactions at such a pace would enable an FI to manage its exposure in real time when a breach or fraudulent transaction occurs.

Second, an improved ability for prediction. Conventional data analysis tools, including linear regression analysis, have generally focused on explanation (causality), but do not provide a particularly good basis for prediction: a regression that may fit a particular data set may not fit well out-of-sample.[40] A statistical model explaining much of a data set may actually be overfit, describing noise instead of the underlying relationships. Machine learning techniques, including decision trees, support vector machines, neural nets and deep learning, have shown that averaging over many small models tends to give better out-of-sample prediction than choosing a single model which may be overfit.[41] This technology may change efforts to counter financial crime: rather than follow transactions and activities ex-post, FIs may be able to predict them and act proactively.

Lastly, specific types of machine learning allow for automated analysis of not just numeric data sets, but all kinds of data sources. Deep learning is being applied for natural language processing to analyze spoken word, and neural networks for automated written text analysis.[42] Systems based on these technologies can automatically analyze information from open sources (such as deep web threat intelligence) and identify fraud in phone calls to FIs, on checks and with credit cards, and ascertain the validity of official documents.

A problem for the application of machine learning for suspicious transactions detection is the need to "train" algorithms using historical data. For the algorithm to learn what distinguishes money laundering from regular transactions, it needs to be trained with historical, final data, with a clear label of which transactions turned out to be "ML" or "non-ML". Unfortunately, such final data is often lacking: FIs typically do not receive feedback from law enforcement agencies on which of their reported activities have turned out to be money laundering. The lack of a universal, clear definition of money laundering and guidelines on how it can be identified also complicate the identification of transactions. After all, FIs report suspicious activity, but not established money laundering transactions, to regulators.

Technologies for "unsupervised learning" may help overcome this problem. Unsupervised learning methods do not need final, labelled data to perform their analysis: the system will learn relevant patterns from the data. This could not only overcome the problematic lack of training data for algorithms in AML, but could also lead to additional insights: unsupervised learning allows one to analyze data without knowing ex-ante what you're looking for – an advantage that could be well applied in the detection of suspicious activities on payment systems, since laundering presents in many forms and develop on a continuous basis.

39 Dan Adamson at "Machine learning – the future of compliance?" panel discussion at Sibos conference, September 28, 2016.
40 Andrew Tiffin, "Seeing in the dark: a machine-learning approach to nowcasting in Lebanon," IMF Working Paper WP/16/56, March 2016.
41 Hal Varian, "Big data: new tricks for econometrics," April 14, 2014.
42 Trevor Hastie, Robert Tibshirani, Jerome Friendman, "The elements of statistical learning," Second edition, 2001, pp. 404-405.

Figure 4. Classification of several analytical methods			
Method		**Description**	**Examples**
"Conventional" statistics		Conventional methods of statistical analysis, requiring full knowledge of applicable situations and high-quality, structured data set.	Linear regression analysis, ordinary least squares, if/then analysis.
Machine learning	Supervised learning	Machine learning is the subfield of computer science that "gives computers the ability to learn without being explicitly programmed."	Parametric/non-parametric algorithms, support vector machines, kernels, decision trees.
	Unsupervised learning	In unsupervised learning, algorithms are required to analyze data without that data being labeled, or the algorithm being trained with example data previously. Self-training algorithms can be deployed to find anomalies, patterns and trends across larger data sets.	Clustering, dimensionality reduction, principal component analysis
	"Deep learning" and AI	The application of multiple layers of ML algorithms (both supervised and unsupervised), emulating the deep, layered learning process of the human brain. Allowing for more complex pattern recognition and analysis of a wide variety of information inputs.[43]	Natural language processing, speech recognition, computer vision.

3. Robotics: automating manual processes and research

Robotics concerns the use of artificial intelligence to automate manual tasks. Different from machine learning, robotics is not so much about the analysis of information, as about the management of processes that were previously run by humans. In AML/CFT and the countering of fraud, analysts still have an important role in the investigative process, bringing together information, and making an informed decision, kicking off further processes. Several FIs are experimenting with robotic control over the process of acting on a money laundering alert and conducting an investigation. Robotics could significantly bring down the cost of compliance by reducing staff needs, and potentially limiting human bias in decision making. Automation also reduces the possibility of misreporting through human error.[44]

4. Shared utilities and the distributed ledger: upgrading AML information sharing

While the above-mentioned technologies all concern upgrades applied within FIs, the larger AML/KYC information sharing and law enforcement architecture of which FIs are part could equally be upgraded with new technologies.

Shared utilities

Financial institutions are already using KYC utilities, repositories in which multiple institutions centrally share or store customer due diligence information. In principle, their centralized nature makes KYC utilities more efficient and faster vehicles of information sharing than the bilateral, ad-hoc information sharing which is default in the current AML/CFT framework. However, liability issues for utility users (which are liable for the data they retrieve), differences in data standards, data gaps and the fact that no utility currently contains all relevant AML/

43 See Najafabadi et al, 2015.
44 Andrew Haldane, "Towards a common financial language," speech at SIFMA symposium, New York, March 14 2012.

CFT-related customer information,[45] limit the usefulness of such utilities.[46] Furthermore, it is unclear to what extent FIs can safely rely upon data obtained from utilities without conducting further diligence, which would undermine much of the benefit of using utilities.

In the longer term, shared applications could also be set up going beyond information sharing vehicles. For example, financial institutions could outsource the ongoing monitoring of payments systems to one shared, central surveillance entity reading wholesale payment systems to detect anomalies. Such an entity would have a more systemic view of fraud and money laundering in the entire financial system, rather than in one financial entity. However, this would require not just an upgrade of technology, but a significant change in the setup of the AML/CFT regulatory framework, which currently designates main responsibility for surveillance to individual financial institutions (see chapter 4).

5. Biometrics and cybersecurity: determining client identity for Customer Due Diligence (CDD) and secure client interaction

Biometrics

Know-your-customer due diligence regulations require FIs to gather personal information on their customers to ascertain their identity and estimate their proneness to money laundering. To that end, records of official documents need to be obtained, their validity determined, or natural persons need to be identified based on their personal traits. Biometrics are now allowing FIs to automate these processes, while improving the accuracy with which an identity or the validity of an official document can be established. Biometric recognition or biometrics refers to the automated recognition of individuals based on their biological or behavioral traits. Examples of such traits include fingerprint, face, iris, palm print, retina, signature, handwriting and voice. Images from sensors are analyzed by applying deep learning algorithms and compared with stored information in a database to establish the individual's identity.

Through the application of biometrics, an FI can ascertain an (onboarding) client's identity through biometrics remotely, rather than requiring the client to visit a bank branch to establish his identity by handing over official identification documentation. FIs are also applying biometrics, together with cybersecurity measures, to secure their interactions with customers.

FIs face several issues when applying biometric technology. First, the accuracy of biometric technologies differs per method, for example, iris scanning is generally more accurate than face recognition. Second, biometric information is very sensitive to the individual concerned, and some organizations have in the past voiced privacy concerns about the use of this information in technological appliances. Given the risk that an individual's biometrics information could be stolen or compromised, it is important that FIs store sensitive biometrical data on secure servers. FIs also combine biometrics with other measures (such as GPS data, as described above) to mitigate the risk of hackers accessing accounts using compromised biometric data.

Cybersecurity and multi-factor identity authorization

As clients are increasingly able to access their product portfolios from their personal

45 For example, DTCC AvoxData provides legal entity data, LexisNexis provides information to help assess risks by way of a list of politically exposed persons and sanctions screening, NORCOM provides criminal data, and agencies like CIBIL, Experian PLC and Equifax Inc provide credit ratings. Source: Tata consulting services, "Reimagining KYC using blockchain technology," white paper.

46 See chapter 5 for further discussion of legal and regulatory issues concerning data sharing and shared utilities.

devices, FIs need to mitigate the risk of fraud and hacking of accounts. Securing interactions between FIs and their customers is a constant innovation race between FIs and fraudsters. Multi-factor identity authorization requires a user to present several separate pieces of evidence to an authentication mechanism before access is granted. Typically, at least two of the following categories would be used: knowledge (something they know), possession (something they have), and inherence (something they are). For example, some FIs now use geolocation (GPS) to establish a client's login location, or send a user an alert when their account is being logged onto. Additionally, new encryption technologies are being applied for secure data transmission.

The distributed ledger as a single source of truth

Distributed ledger technology, whose potential has been widely documented,[47] has particular attributes for securely and instantaneously accessing and sharing information that could in the longer term serve to solve some of the issues concerning information sharing between banks and law enforcement authorities.

DLT provides a single source of truth by requiring that any change in the database be verified by a majority of nodes, or entities that constantly update the database. That requirement provides security, since a hacker would have to control the majority of the nodes in order to effectively manipulate the database. Permissioned distributed ledgers enable rapid, real-time transactions as there is inherent trust between the nodes, eliminating the need for large amounts of computing power to deliver proof of work. In the long term, KYC utilities could be placed on a distributed ledger, with participating financial institutions and law enforcement agencies acting as nodes. Logically, a permissioned distributed ledger would be the only option for such use, as access to the database should be limited to entities with AML/KYC obligations under the FATF framework.[48]

Placing KYC utilities on a distributed ledger could allow FIs to share sensitive consumer data across several entities without compromising nonpublic, personal data – although it would not solve all of the issues concerning data sharing. First, as mentioned above, it would be hard to hack or manipulate due to the need to control a majority of nodes. Second, when the data on the ledger is combined into a cryptographic hash function, the ledger would only convey sensitive personal information if the accessing party enters the same hashing functions.

DLT could also serve as a safe repository for unique identifiers for transactions, legal entities and clients. As explained in chapter 4, assigning a unique identification code (such as the LEI) to legal entities and clients making use of the financial system would assist AML/KYC procedures by allowing for the unambiguous identification of (parties to) a transaction, subject to the agreed reliability of the identifiers (how often identifiers are verified or renewed).

47 See IIF, "Banking on the blockchain: Re-engineering the financial architecture," November 2015; IIF, "Getting smart: contracts on the blockchain," May 2016. A thorough introduction to the distributed ledger is given by Ali, Barrdear et al, "Innovations in payment technologies and the emergence of digital currencies," Bank of England Quarterly Bulletin, 2014 Q3, pp 262-275.

48 Credit Suisse, "RegTech: how a new wave of technologies is transforming the regulatory and compliance landscape for financial institutions," Washington White Paper, November 2016.

Figure 5. Key solutions for AML/KYC compliance and their underlying technologies	
Key solutions areas	**Underlying technologies**
1. Security solutions for unambiguous identity verification and bank-client interaction	Biometrics combined with deep learning; cryptography, distributed ledger technology
2. Automated detection of suspicious behavior on payments and client systems	Machine learning, artificial intelligence
3. Big data infrastructures: data ingestion, storage, visualization and analysis	Increased computing power, improved and cheaper data storage, faster data connections, cryptography, topology, artificial intelligence
4. Automated execution of AML/KYC investigations: analysis of internal and external data sources	Robotics and AI, big data infrastructures
5. Shared utilities and centralized data repositories	Cryptography and, in the future, possibly distributed ledger technology

CHAPTER 4 – PREPARING FOR THE FUTURE: AN AGENDA TO PROMOTE TRANSFORMATIVE TECHNOLOGIES FOR BETTER COMPLIANCE

In the discussion of new technology to be applied in AML/CFT, several barriers to the implementation of new technology in the financial sector have been identified. This chapter takes stock of ways to overcome barriers and facilitate the implementation of regtech. It will first focus on regulation and legal issues. In several areas, updates and changes to regulation could benefit the adoption of regtech for AML/CFT:

1. Close gaps in the international AML/CFT framework

As discussed, the current AML/CFT regulatory framework's combination of ambiguity of definitions and guidelines with perceived zero-tolerance enforcement is stifling innovation and leading to overreporting, as FIs become risk averse in the face of hefty penalties. Thereby, the current framework's one-on-one model of information sharing is highly inefficient and poorly suited to the dynamic character of money laundering and fraud. The framework needs to be updated in several aspects:

a. Providing clear, universally agreed definitions and guidelines of key regulatory concepts, such as what constitutes money laundering including primary offenses, or other types of fraud. Also, requirements for FIs should be very clear and confirm non-applicability of "know your customer's customer".

   Universal definitions and standards for key regulatory concepts in the international AML/CFT framework are currently missing. Standard setting bodies including the FATF, the Financial Stability Board (FSB), the CPMI and the BCBS should work together with national data regulatory bodies to create common technical standards that digital onboarding techniques should meet. Also, they should work to create a common understanding and alignment on the type and depth of KYC information that could be exchanged by financial institutions.

b. Improve the quality and timeliness of feedback and response from authorities on FIs reporting to allow institutions to learn, improve procedures and provide them with the ability to "train" technology to recognize patterns and activities of financial crime.

c. Improve information sharing in the AML/CFT system so data is shared more effectively within financial groups, with the authorities, and among peer banks (including on a cross-border basis) to allow a systemic view of financial flows and activities in the international financial system.

Ultimately, the use of regtech in combination with updated, clearer and more appropriate rules on information sharing could lead to a system abandoning the Suspicious Activity Report as a central data reporting mechanism. Instead, it could allow law enforcement agencies to access AML/CFT data on a continuous, automated basis, for example by running algorithms across different FI data pools. This would allow law enforcement agencies to act based on a specific request of their own, or to act based on alerts from its own automated systems, and from a system-wide point of view. Alternatively, standardized utilities shared among multiple FIs could already bring economies of scale and systemic policing of financial infrastructures. More information on this topic can be found in the IIF's regulatory comment letters on AML/CFT.[49]

49 See www.iif.com/advocacy/comment for more information. Two recent submissions to regulators on data sharing for AML/CFT have been: IIF, "Re: FATF consultation of the private sector on correspondent banking," Letter to FATF, Washington DC, August 5, 2016; and IIF, "Re: Facilitating effective sharing of AML/CFT information," Letter to FATF, Washington DC, May 25, 2016.

2. Improve data quality and data sharing policy

Improved data quality and sharing would allow authorities and FIs to obtain a more accurate, granular, up-to-date and potentially systemic view of suspicious activity on financial sector infrastructures. Availability of more and higher quality data would improve the quality of analyses, the robustness of suspicious activity surveillance, and the ability of FIs and law enforcement agencies to automate compliance, reporting and investigation processes. Reforms should address the ability to share data between FIs, among subsidiaries within the same group, and between jurisdictions; and the quality of data, which should be improved through standardization and granular and harmonized definitions.

a. Data sharing

Improving data sharing does not just require changing the information sharing model in the AML/CFT regulatory framework, as that would only address sharing between institutions and regulators. Essentially, as one of the Regtech Working Group participants has stated, "local law is [still] everything" in data policy. Jurisdictional laws typically prohibit FIs from sharing data even between subsidiaries in the same group, between subsidiaries and the holding company, or between activities in different jurisdictions. This inhibits FIs from obtaining a group-wide view of illicit financial flows. To address these issues, the following should be considered:

i. Governments around the world should work to find an appropriate balance between privacy and law enforcement goals in data sharing legislation and policy. While it is of vital importance that governments work to assure the privacy of individuals, the trade-off between assuring privacy and disclosing information needed for wider legitimate use depends significantly on the reasons for which the data would be disclosed. The trade-off between protecting privacy and allowing corporations such as social networks to share information for commercial reasons is radically different from a context in which personal data is shared to counter money laundering and terrorism financing. Policies intended to protect privacy should be tailored to the context in which these sensitive data would be used.

ii. Therefore, any government policy on data sharing and privacy should take into account the latest technological advances. As is argued below, data technologies and encryption techniques such as distributed ledger technology, secure multiparty computation, and hashing have significantly changed the ability to share data centrally across multiple actors while minimizing any sensitive information compromised the discussion in chapter 3 on DLT, and below).

iii. At the broadest international level, the FATF should work to improve the effectiveness of its member states' information sharing regimes. Specifically, as the FATF Recommendations[50] offer a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, the IIF believes that the Recommendations would benefit from clearer guidance to enable more effective information sharing for the reasons noted in this report. Specifics on changes to the Recommendations were noted in the IIF Survey on Financial Crime Information Sharing.[51]

50 FATF, "The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation," February 2012.
51 IIF, "Financial Crime Information Sharing Survey Report," February 2017.

iv. A greater focus should be placed on enhancing national and multilateral programs for the financial sector and government to exchange and analyze intelligence to prevent, detect and disrupt money laundering and broader economic crime threats. Enhancements should be made to legal structures that would allow and encourage development of collective anti-money laundering detection capabilities to generate increased prevention and disruption opportunities against illicit conduct in countries around the world.

v. Public sector bodies should act in FATF to institutionalize analysis of country laws and regulations which may impede the effective sharing of financial crime related information, and establish and promote among member countries international norms for consistent legislation or regulation (and interpretation thereof) where possible.

b. Improving data formats and standardization

As information analysis becomes increasingly automated, there is a need to improve the quality of data shared between countries, institutions and systems:

i. Standardization of data formats is key to enhance data sharing by enabling integration and helping address coordination challenges posed by regulatory fragmentation.[52] Data standards are documented agreements on how to define, represent, format or exchange data. Data standards should be flexible in order to be technology-agnostic, and global in nature. Fortunately, the FSB's Correspondent Banking Coordination Group has recognized the importance of standardization.

ii. Strengthening the adoption of FATF Recommendation 16 on Payments Data Quality. Data quality either needs to be improved by universal adoption of FATF 16, or more investments are required to use the existing data taxonomies with a universal data dictionary.

iii. Applying unique identifiers such as the LEI (which was originally developed for derivatives transactions)[53], the UTI and the Unique Product Identifier (UPI) can help financial institutions and supervisory and law enforcement authorities to unambiguously identify financial institutions taking part in a transaction. Payments on the global payments network are currently routed from/to FIs using bank identified codes (BICs). However, these are not applied at the legal entity level, and an entity can have multiple BICs. In contrast, the LEI is unique and exclusive. The CPMI has advocated that the LEI be included in payment messages, in order for parties to a financial transaction to be easily identified.[54] An effective coding system for unambiguous identification would facilitate automation of transaction surveillance.

iv. In various ways, LEI/UPI/UTI or similar identifiers could be included either in currently used MT format, or on the ISO 20022-compliant MX message format which will be used in the future.[55] In the long term, the AML/CFT enforcement system could benefit from a LEI-type of unique identifier also being applied to non-financial corporate clients of FIs.[56]

52 Office of Financial Research, "Financial Stability Report," Washington DC, 2015.
53 The LEI (SIO standard 17442:2012) is a 20-digit alphanumeric reference code for the purpose of unambiguously identifying legal entities that engage in financial transactions.
54 Alexander Karrer at IIF AMM panel on "The future of AML and de-risking".
55 CPMI discusses the usage of the LEI in payment messages in more detail: CPMI, July 2016, pp. 24-27 and 38-39.
56 To that end, attention should be paid to current issues relating to the governance of the LEI, including the responsibility for creating the identifiers

v. Standardized translation between different scripts: Identification of natural persons can, in the current system, lead to problems when names are translated from one script to another, such as from Arabic or Chinese to Latin script. Creating a global, unique identifier of natural persons would overcome these challenges but likely lead to privacy problems, as this would require a central repository accessible from all jurisdictions containing client identities.

3. Create a proper environment for regtech experimentation

The current AML/CFT framework combines ambiguous guidelines and a lack of universal definitions of key concepts on the one hand, with application by law enforcement agencies of what appears to be a zero-tolerance approach to reporting failures at FIs on the other. Such a supervisory climate discourages experimentation with new technologies (for instance, applying machine learning for money laundering detection) because those systems could underperform unexpectedly and it is difficult to predict what enforcement authorities will consider with hindsight to have been adequate diligence. It is vital that FIs have appropriate supervisory room to experiment with new technologies and, consistently with a risk-based approach, make their own considerations in applying AML/CFT policy.

To mitigate the risk of experimenting with, and migrating to new technologies, regulators could work to enable a "safe" environment for experimentation in which FIs would feel comfortable sharing information about compliance challenges and difficulties in a way that is not detrimental to their relationships with compliance and enforcement authorities, while respecting their commercial status as competitors. This can be done through a number of means:

a. Establishing clear rules of engagement, such as the Chatham House Rule, and general rules for usage of information;

b. Public statements by senior enforcement officials, utilizing global standard setters (FATF, CPMI, FSB, EU);

c. Proactive implementation of a "sandbox" approach for regtech, in which FIs can test new technologies in compliance and reporting in a controlled environment without risk of non-compliance for technical reasons.

Financial institutions can equally promote the adoption of regtech. As members of the IIF Regtech Working Group have noted, procurement procedures at FIs tend to favor incumbent vendors by requiring extensive track records. New entrants to the market offering new tech solutions by definition lack such track records and tend to be disadvantaged in the procurement process.

FIs also face a challenge in integrating new technologies within their existing IT infrastructure, which often consists of a complex combination of legacy technologies. Some have suggested that FIs could set up a "big data" infrastructure parallel to their existing IT systems, providing the platform on which other applications run. FIs could set up a two-speed IT architecture consisting of a decoupled reliable back-end (the legacy systems) and a flexible, agile front-end consisting of the new "big data" infrastructure.[57]

at a specific timing of the transaction, for paying the cost, owning the intellectual property, overseeing the sharing of information across jurisdiction, etc.

57 See chapter 3, section 1.

4. Shared utilities should be able to carry responsibility and liability

Shared utilities will only be able to operate effectively and independently from individual FIs if, rather than the FIs, the shared utilities can carry responsibility and liability for the information they contain or the activity they execute. The BIS's CPMI has acknowledged that "banks should have some assurances from relevant authorities... with respect to the appropriateness of and reliance upon any [KYC utility] for the purposes of AML/CFT compliance."[58] Banks commonly report that KYC utilities currently have very limited added value to them. Since the bank will carry the liability for the information retrieved from a third party when reported to law enforcement agency, it will need to double-check that information, including from shared utilities. Banks need to have clarity on when and to what extent they can rely upon information drawn from utilities. Serious consideration should be given to establishing international standards or sound practices for such utilities to create greater assurances of achieving official AML/CFT goals.

5. Make regulation and supervision resilient to continuous technological innovation

Authorities need to ensure that regulations and supervision are resilient to continuous technological innovation, remaining reflective on how regulated activities are carried out in practice. Innovations can materially change the nature of a regulated activity, including associated risks. Regulatory frameworks should reflect that, or they risk becoming obsolete or based on out-of-date assumptions. They should allow proper leeway and flexibility for FIs to apply and try out new technologies and practices, while ensuring that prudential and conduct risks remain adequately identified and addressed. Below, we discuss several supervised activities subject to innovation as examples.

a. Machine learning has the ability to create more accurate models of money laundering risk (or other types of risk, including credit or market risk) with greater predictive power than conventional models. However, these models differ in nature from those created with conventional statistical methods. No longer will FIs have a set of standard scenarios with statistically defined thresholds; instead, machine learning creates dynamic systems that learn and adjust based on continuously incoming data. Supervisory practices will need to adjust accordingly to allow these technologies to be applied, starting with supervisors building capacity to understand and work with them.

b. Customer identification is another example. Even though technologies for online identification have become precise and secure, many jurisdictions still require customers to identify themselves in person and sign on paper in order to open an account or for a transaction to be legally binding. This stifles the application of new ways of onboarding and due diligence.

c. Data policy should adjust as innovations change the nature of data sharing and storing to alter the trade-off between efficient use of data and protecting privacy. For example:

   - Decentralized data repositories which are now in vogue can distribute fractions of data across many locations. As a result, a file is stored in no jurisdiction in particular, thus improving security while still being centrally accessible for authorized personnel. Yet this data model may appear to contravene data localization, data privacy and data processing requirements in current

58 CPMI, July 2016, p. 2.

regulations.

- New cryptographic tools including secure multiparty computation, blockchain and hashing offer new ways to share data while retaining individual privacy, but the flexibility such tools provide is yet to be recognized in regulations, thus impeding their uptake.[59]

Policymakers should continuously reassess the impacts of technological developments on data security, usage and privacy, ensuring that regulations strike an appropriate balance between protecting privacy, other policies and effective data use for AML/CTF purposes.

6. Change supervisory focus as automation alters the nature of risk in the financial sector

Authorities should change their supervisory focus as the business model of FIs changes through automation – and risks inherent in the business model adjust accordingly. Digitization will likely improve and speed up compliance practices and decrease human error and bias. At the same time, model risk and cyber risk may become more pronounced.

a. Model risk - As McKinsey has noted, "increased data availability and advances in computing, modeling, and algorithms have expanded model use. However, errors from suboptimal models can lead to poor decision making and increase banks' risks. Errors in models stem from issues with data quality, conceptual solidity, technical or implementation errors, correlation or time inconsistencies, and uncertainties about volatilities. Some banks have experienced model-risk-related losses. Regulators could focus on mitigation strategies, including more rigorous, sophisticated model development, or better execution (with higher-quality data), thorough validation, and constant monitoring and improvement of the model."[60]

b. Cyber risk - Banks' are increasingly relying on software, systems and data in key business processes, and on IT infrastructures that are open and connected to the internet. That makes them vulnerable to cyber attacks. These not only put the banks' operational continuity at risk, but also the confidentiality of customer data. FIs are investing heavily in more resilient infrastructures, and are working together to counter cyber risks in forums including FS-ISAC (Financial Services Information Sharing and Analysis Center).

59 Mark Flood, Jonathan Katz, Stephen Ong and Adam Smith, "Cryptography and the economics of supervisory information: balancing transparency and confidentiality," September 4, 2013.
60 McKinsey and Company, "The future of bank risk management," McKinsey working papers on risk, December 2015.

Fig. 6. Overview of IIF regulatory recommendations on applying regtech in AML/CFT	
Recommendation	**Relevant authority**
1. Close gaps in the international AML/CFT-system	
a. Provide universally agreed definitions and guidelines on key regulatory concepts	FATF
b. Provide FIs with feedback on their reporting whenever possible	Local law enforcement agencies; supervisors
c. Find an appropriate balance between privacy and law enforcement goals in data sharing policy	National governments, EU, data policy agencies
d. Policy on data sharing and privacy should take into account latest technological advances	National governments, EU, data policy agencies
e. Change the setup of information sharing in the AML/CFT system	FATF with support of member jurisdictions, involving data policy authorities and national prudential and conduct supervisors
2. Improve data quality and data sharing policy	
a. Data sharing policies	FSB, FATF should mandate action to member jurisdictions
b. Improving data quality	
i. Standardization of key data formats	Suspicious activity reports: local law enforcement agencies, working through FATF Payment system messages: CPMI, SWIFT, financial institutions
ii. Strengthening the adoption of FATF Recommendation 16 (Payments Data Quality)	FATF member jurisdictions FATF: conducting mutual evaluations
iii. Embedding unique identifiers in transaction data for unambiguous identification of transaction parties	CPMI and SWIFT; BCBS
iv. Standardize translation rules between different scripts to avoid confusion on names in non-Latin script	FATF
3. Create a proper environment for regtech experimentation	
a. Establish clear rules of engagement	FATF: statement on proportionality of sanctioning under the risk-based approach;local supervisors; local law enforcement agencies
b. Public statements by senior enforcement officials and global standard setters	National prudential supervisors, FATF, CPMI, FSB, BCBS
c. Sandboxes for regtech implementation	National prudential and conduct supervisors
Financial institutions adjust procurement processes to allow new market entrants an equal chance	Financial industry; regulators to review outsourcing standards and other regulations that drive FIs toward highly formalistic requirements.
Promote innovation and experimentation of financial institutions with regtech	Local regulatory and law enforcement agencies: • Dialogue with FIs on application of new technologies and required leeway • Dialogue between law enforcement and regulatory agencies to assure consistent policies, avoid unpredictable enforcement
4. Shared utilities should be able to carry responsibility and liability	Local law enforcement agencies, governments; FSB and FATF standards to encourage consistent action
5. Make regulation and supervision resilient to continuous technological innovation	Various public authorities, working based on international standards (BCBS, FATF, FSB)
6. Change supervisory focus as automation alters the nature of risk in the financial sector	National prudential and conduct supervisors, working based on international standards (BCBS, FATF, FSB)

Questions or comments regarding this publication may be addressed to:

Kristen Silverberg
Managing Director
ksilverberg@iif.com

Andrés Portilla
Managing Director,
Regulatory Affairs
aportilla@iif.com

Bart Van Liebergen
Associate Policy Advisor
bvanliebergen@iif.com

Stephanie Van den Berg
Program Associate
svandenberg@iif.com