



EVOLVING AML JOURNEY

**LEVERAGING MACHINE LEARNING
WITHIN ANTI-MONEY LAUNDERING
TRANSACTION MONITORING**

Artificial Intelligence (AI) and one of its key components, Machine Learning (ML) are innovative and disruptive technologies that are widely used within many industrial sectors, including life sciences, automotive, aerospace and defense.

However, despite numerous potential applications within the financial services sector, specifically within Anti-Money Laundering (AML), adoption of AI and ML has been relatively slow. This has been, in part, due to the following: (1) limited comprehension of the application of AI and ML within AML compliance programs; (2) the notion of ML being a “black box” where the inner workings are not clearly understood by regulators and compliance officers; and (3) the cautious approach taken by regulators requiring compliance officers to understand and validate how outcomes from AML models are arrived at.

Nevertheless, when coupled with hybrid models involving human resources supported by AI, AML solutions can be developed that provide significant benefits, including a reduction in compliance costs and improvements in the transaction monitoring process leading to greater overall efficiency.

ML APPLICATIONS FOR AML TRANSACTION MONITORING

AI is a field of computer science focused on the development of computers to carry out activities typically executed by humans, specifically activities requiring humans to take decisions and rely on their intelligence.

There are several component technologies within AI all with numerous applications. For example, Natural Language Processing (NLP), through which computers process human language, is used for translating payments in payment screening, processing mortgage applications and negative news screening (see Figure 1).

ML is a sub-field of AI where computers are able to learn when exposed to new data without being explicitly programmed. The potential applications for this within suspicious activity monitoring and Transaction Monitoring (TM) are vast.

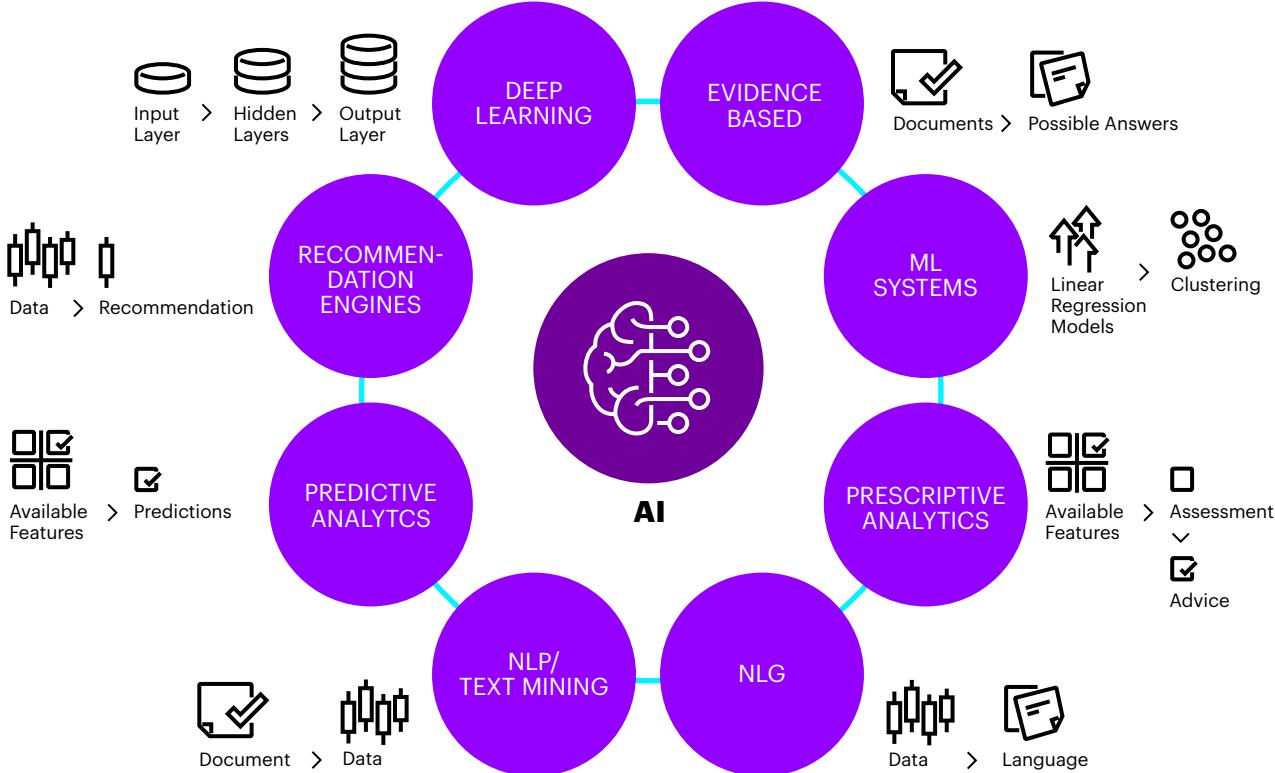
A common TM challenge is the generation of a vast number of alerts requiring costly operations teams to triage the alerts. With increasing customer numbers, and increasing numbers of transactions, TM alert volumes have increased significantly at financial institutions (FIs). This increase in alerts has resulted in an upsurge in the number of personnel required to triage and process them. However, in leveraging ML at the alert triage stage, alerts can potentially be suppressed, hibernated (set aside for later examination) or even, at some time in the future, closed automatically.

ML can teach computers to detect and recognize suspicious behavior and classify alerts following a risk-based approach as being of high, medium or lower risk. Applying rules to these alert classifications can facilitate hibernation and auto closure of alerts, allowing human resources to supervise machines that triage these alerts rather than reviewing alerts manually. This change is illustrated in Figure 2.

Machines can be taught to recognize, score, triage, enrich, close or hibernate alerts. This can help focus experienced human resources on complex problems while computers perform simpler tasks for them. By using AI across the entire TM process, alerts can be auto-triaged leveraging ML; they can be auto-enriched with account, transaction, and customer information from external and internal data sources leveraging intelligent automation and NLP; and narratives for Suspicious Activity Reports (SARs) can be auto-generated using Natural Language Generation (NLG). Institutions leveraging AI in this way can reduce dependencies on human operators to perform routine tasks, reduce the total time it takes to triage alerts, and allow personnel to focus on more valuable and complex activities.

Figure 1. Illustration of some AI Applications and Components

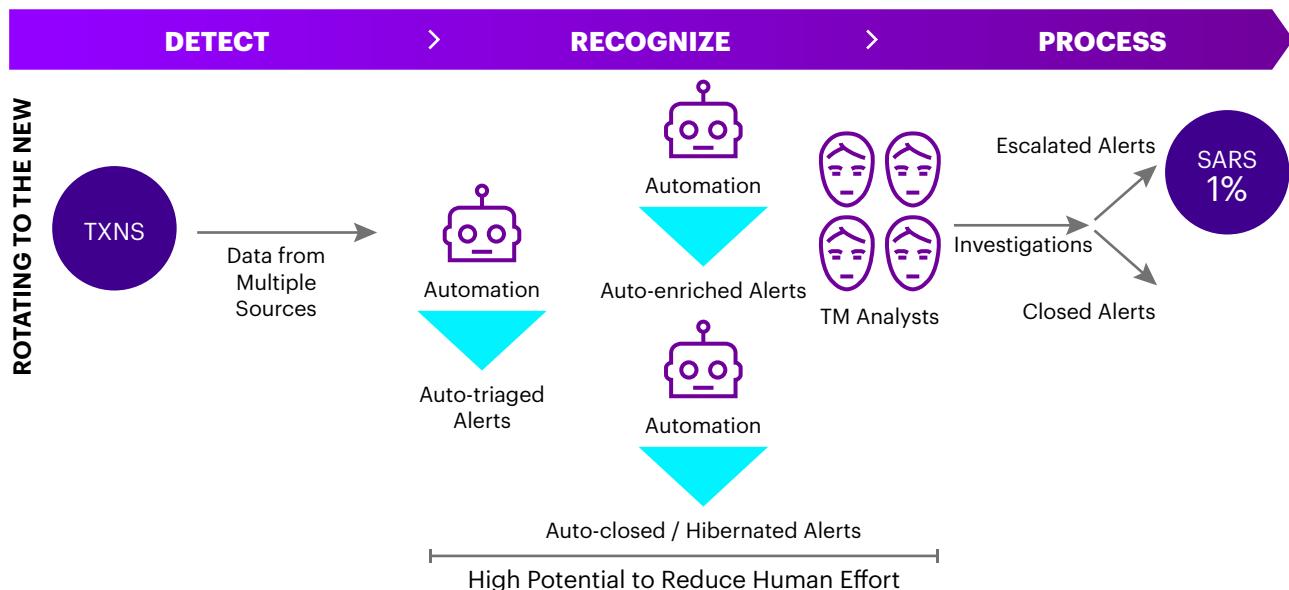
Other components include, Genetic Algorithms and Swarm Intelligence. This document largely focuses on ML for AML TM.



Source: The Artificial Intelligence Ecosystem, Narrative Science

Figure 2. Introducing ML into AML TM Alert Triage

With the introduction of ML into AML TM alert triage, SAR conversion rates should improve from the current unacceptable rate of ~1% in the banking sector.



Source: Accenture, September 2017

CHALLENGES TO IMPLEMENTING ML

Through Accenture's work with global FIs we have identified a number of implementation challenges for financial services firms seeking to implement ML as part of AML TM solutions.

Figure 3. The Challenges to Implementing ML as part of a TM Solution



Source: Accenture, September 2017

These challenges include poor data quality, low Know Your Customer (KYC) profile refresh rates, lack of a holistic view of the customer, limited knowledge of both financial services and ML, regulatory expectations and appetite, and lack of straightforward processes to follow for implementation.

1. Data quality management and profile refresh.

Data Quality Management (DQM) is a required activity for all monitoring systems and analytics. It is not unique in any way to ML applications. Both static files, for example KYC files, and dynamic data held by FIs on their customers' transactions have seen low completeness ratios in areas such as missing payment information and high error rates in recent years. Additionally, there is also a general lack of data traceability and data lineage.

Some FIs address data issues on an alert and/or profile basis when alerts are generated as false positives or noise. This method reduces reoccurrence of noise or false positives. However, others prefer large-scale, one-off data reconciliation/refresh exercises. During the last few years, many FIs have undertaken large and costly data remediation projects to improve data and have implemented frameworks to manage data quality. However, data quality remains an ongoing problem. To the challenge of missing and outdated data, there is an opportunity to tie profile refreshes into sales and marketing exercises. Relationship managers can use profile refresh opportunities to reach out to their customers and identify cross-selling opportunities.

2. Lack of a 360-degree view of the customer.

Another challenge in implementing ML-supported TM programs is the inability for FIs to build a 360-degree view of the customer. For example, financial services firms do not have the global freedom to share information about their customers to build a comprehensive network. Furthermore, FIs do not formally collaborate on AML as this is a cost. Building a 360-degree view would require collaboration across FIs and information agencies that does not exist today.

Currently, once FIs decide to file an SAR and submit it to the regulator, there is limited feedback and intelligence returned. In addition to sharing information securely between FIs and regulators, external (to KYC) data sets can be used in areas such as marketing data, which has rich datasets on customer behavior not generally used for AML behavior modeling and alert enrichment and/or triage. However, there have been some developments in recent years that are paving the way to alleviate this challenge of data sharing. Regulators are increasingly leaning toward data sharing between banks. Relevant regulations encouraging data sharing are US Patriot Act 314 a and 314 b and PSD2. The UK Treasury is also encouraging sharing of data via an Open Banking API/Open Banking Working Group. However, data ownership, medium (e.g. cloud) and the extent of this data sharing needs to be defined. It is a matter of time before large amounts of transactional data will become available on intrabank data clouds.

3. Limited knowledge of both financial services and ML. Another reason why ML has not been as widely applied within the financial services industry is that very few people are experts in both ML techniques and financial services. As a result, there have been fewer applications targeting financial services problems from start-ups and established vendors, limiting acceptance of ML within the financial services sector (especially for financial crime prevention).

4. Limited regulatory appetite. FIs have held back from implementing ML solutions because regulators expect models that can be clearly understood. They typically insist that all choices, limitations, and results be documented before such models are implemented. In the regulators' view, the models should be designed in a way that allows for results to be reproduced given the same input data. This is not always possible with ML algorithms.

Additionally, there is some evidence that large vendors are, in effect, acting as leading regulators. This is because some regulators recommend specific solutions for TM that are ineffective and generally need to be replaced by intelligent and adaptive solutions. These large players dominate the technology space and, consequently, there is only a narrow field of play for start-ups. Start-ups tend to need support from consultancies and other third parties that help banks with their evaluations and implementations.

5. Lack of straightforward processes.

ML is a relatively new technology and there are few established, straightforward processes to follow to implement it. Without knowing what to look for, teaching systems to detect certain types of financial crime can be tricky. For example, how does one teach a system to recognize terrorist financing? There is a carousel process for fraud but nothing similar for terrorist financing (nothing, that is, other than name matching against terrorist lists). While some of these problems are better suited to unsupervised learning, model validators should be sure about the desired outcomes.

MODEL VALIDATION AND BLACK BOX TECHNIQUES FOR ML AML MODELS

Any statistical model chosen by an FI for TM needs to follow steps similar to those illustrated in Figure 4.

These steps are recommended by the Office of the Comptroller of the Currency (OCC) for model risk management.¹ Extensive documentation is required for models selected and the regulators expect FIs to be able to re-create results and explain exactly how their models work.

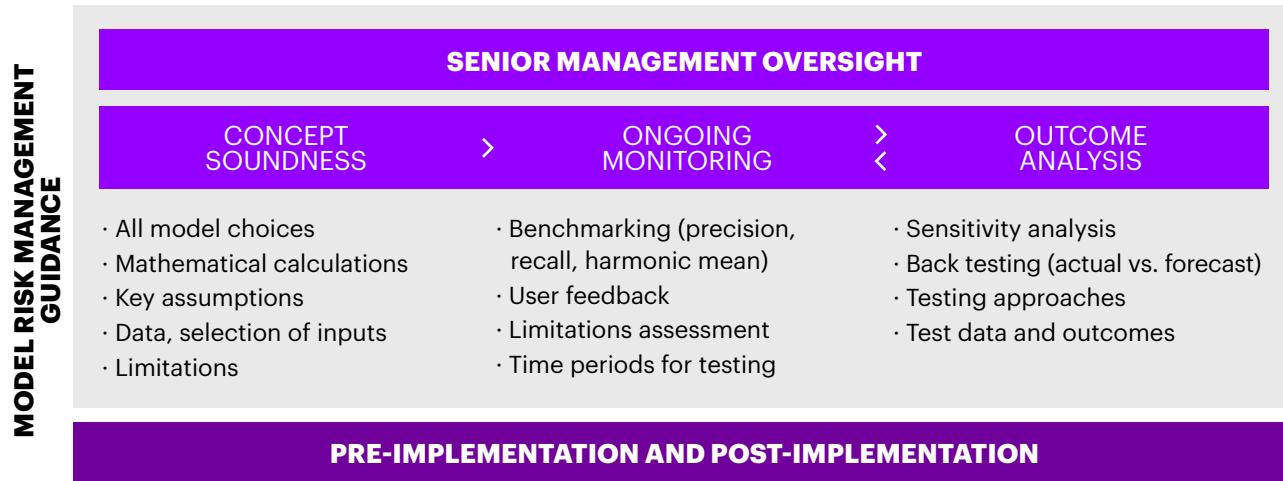
The introduction of ML opens up numerous new techniques for TM, all constructed with mathematical equations. Some of these algorithms or techniques are simpler to understand than others. Simpler algorithms include decision trees while more complex algorithms may comprise neural networks.

Algorithms that are predictable, traceable, and simple to explain are “white box” techniques. On the other hand, more complex algorithms are known as “black boxes,” as the mathematical calculations underlying these techniques are far too dense and complex to be able to recreate results and provide rationale for the learned parameters (such as weighting). Figure 5 illustrates how model validation becomes more complicated as techniques move from “white box” to “black box.”

Currently, there is no straightforward method to validate complex or black box ML model choices for internal auditing and for external regulatory purposes. Black box ML techniques can be tested by adopting (and adapting) the Turing test, whereby human analysts are trained with the same samples as machines and an observer evaluates results to determine precision and recall. At the same time the observer needs to determine which results were produced by a human and which were produced by an ML system. This process could be undertaken as an interbank activity, possibly with the involvement of regulators.

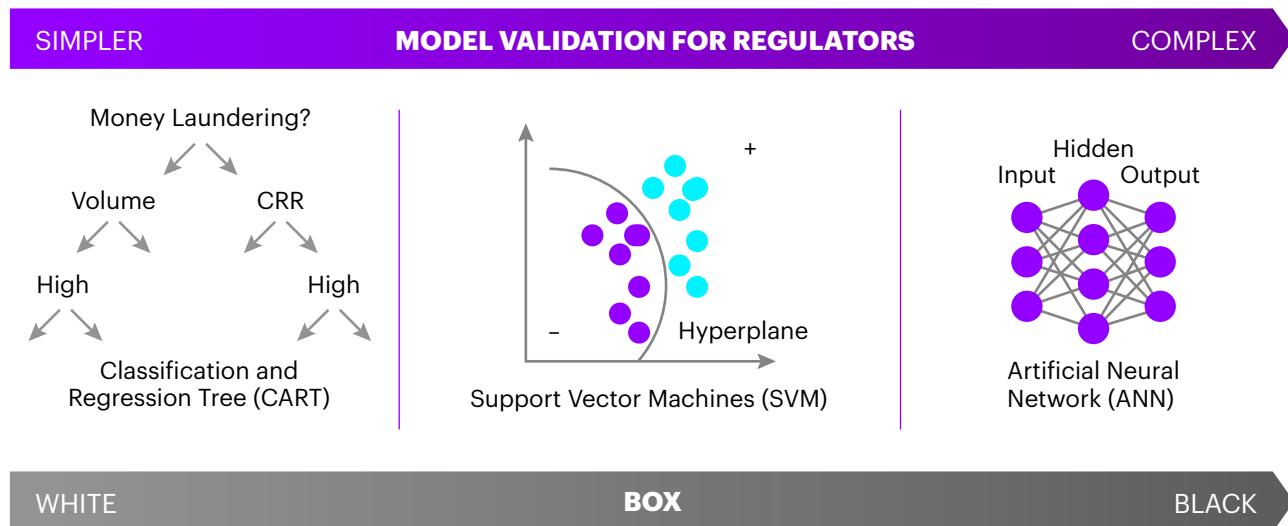
However, just as current TM systems require their scenarios and segments to be updated, ML-based TM systems will also have to be updated periodically. This can be more complicated than standard TM system maintenance and ongoing testing is required. Realistically, such testing and updating should be consultancy or vendor driven as part of an ongoing maintenance contract. The slightest change in the type of data that once produced desired results can render the system unreliable.

Figure 4. Summary of Model Risk Management Guidance from the OCC



Source: Supervisory Guidance on Model Risk Management, Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency

Figure 5. Complexity Scale for Model Validation of ML Algorithms



Source: Accenture, September 2017

HOW ACCENTURE CAN HELP

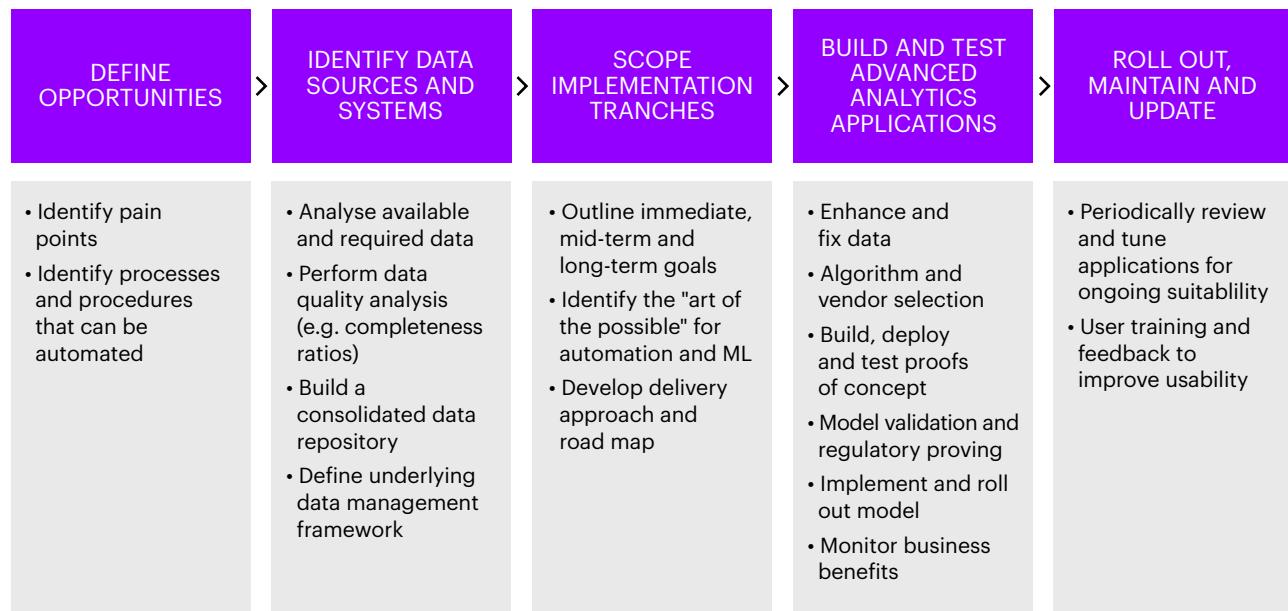
Accenture provides services to global FIs to implement both ML and robotic process automation (RPA) programs.

We have extensive capabilities in this area, including analytics and digital centres of excellence and subject matter specialists to:

- Identify and analyze business opportunities
- Assess the impact of possible solutions (such as updating procedure manuals versus adopting ML)
- Deliver innovative bespoke and industry leading technology solutions, including implementation of TM systems, AML model validation, and operating model transformation to improve the human and virtual workforce

We have vendor alliances, both with Fintech start-ups² and with leading firms. Accenture consultants meet on a regular basis with new vendors, help vendors build their capabilities in the financial crime prevention space, and evaluate them to deliver greater value to clients. Within the financial crime space, Accenture has established an effective and efficient methodology to allow our clients to meet regulatory expectations and reduce volumes of TM and Name Screening alerts. This methodology is illustrated in Figure 6 below.

Figure 6. Summarized Steps for Rapid Benefits Realization from ML and RPA



Source: Accenture, September 2017

Within the financial crime space, Accenture has established an effective and efficient methodology to allow our clients to meet regulatory expectations and reduce volumes of TM and name screening alerts.

CONCLUSION

Many banks have started implementing business process automation in the form of RPA and see AI and particularly ML as the next step in the journey to greater efficiency and effectiveness. Some banks, however, believe they should walk before they run, meaning that robotics solutions should be in place before AI ML solutions are considered.

In fact, robotics and AI ML can exist independently of each other and each can support the other's capabilities. Robotics can be used to train AI ML models and AI ML models can be used to add decision-making (in the form of NLP) or reading (via optical character recognition) capabilities to robotics models.

The appetite for automation is increasing rapidly, but challenges remain. Implementing ML may improve event-to-SAR conversion rates but there will always be a need for human involvement. Hybrid human/AI models are likely to appear in the near future and should represent the next generation of AML TM alert operations teams. The adoption of ML and, ultimately, AI in AML is only the beginning of financial services compliance and resilience automation.

ABOUT THE AUTHORS

Samantha Regan

Samantha is a Managing Director, and is the North America Lead for the Regulatory Remediation & Compliance Transformation group within Accenture's Finance & Risk practice. Based in New York, she has 17 years of global experience working with C-suite executives and their businesses in compliance and regulatory initiatives.

Heather Adams

Heather is a Managing Director, Accenture Finance & Risk. Based in London, she leads Accenture's UK & Ireland Resilience team, developing capabilities and supporting clients in their efforts to be resilient to a range of external and internal threats, including financial crime. Heather has extensive experience in delivering large-scale complex business change for banks and has worked with senior leaders to define and implement financial crime risk strategies to drive high performance.

Philippe Guiral

Philippe is a Senior Manager, Accenture Finance & Risk, based in New York. He leads Accenture's North America Financial Crime Group, and has over 12 years of experience, defining capabilities and strategies to support clients in their financial crime prevention programs in both the UK and the US. Philippe specializes in delivering large-scale complex business and technology financial crime change programs to drive high performance.

Saad Choudri

Saad Choudri is a Technology Consulting Principal, Accenture Finance & Risk, based in London. Saad has over 12 years of international multisector experience as a change professional with a special focus on financial crime prevention and artificial intelligence.



The appetite for automation is increasing rapidly, but challenges remain. Implementing ML may improve event-to-SAR conversion rates but there will always be a need for human involvement.

REFERENCES

1. "Supervisory Guidance on Model Risk Management," Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, April 4, 2011. Access at: <https://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf>
2. FinTech Innovation Lab, London: <http://www.fintechinnovationlablondon.co.uk/>

ACKNOWLEDGMENTS

The authors would like to thank the following Accenture employees for their contribution to this document:

Garikai Mparutsa

Zhana Gali

STAY CONNECTED

Accenture Finance and Risk

www.accenture.com/financeandrisk

Finance and Risk Blog

financeandriskblog.accenture.com/



Connect With Us

www.linkedin.com/showcase/16183502/



Follow Us @AccentureFSRisk

www.twitter.com/AccentureFSRisk

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is www.accenture.com

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.



1 2 4 6 0 5 6 9