CAPCO

JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

SECURITY

Setting a standard path forward for KYC

ROBERT CHRISTIE

DIGITIZATION

#47
04.2018

JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

ORGANIZATION

CURRENCY

SECURITY

Setting a standard path forward for KYC

ROBERT CHRISTIE | Principal Consultant, Capco

ABSTRACT

Customers have a good reason to be upset with banks over their KYC processes, which tend to be complicated and costly. Given the pressure and timelines from regulators, it is understandable that banks have struggled to make KYC customer-friendly. With new technologies becoming rapidly available, now is the perfect time to set a new standard for eKYC solutions that would make compliance fast and cost-effective to implement. However, there is a key dependency that needs to be considered before a global solution can be delivered. This article provides some recommendations on how this could be achieved.

1. INTRODUCTION

Since 2001, regulatory bodies across the world have introduced a wide array of regulations targeted at the opening and maintenance of bank accounts by individuals and corporates. This increase of regulatory scrutiny had arisen from increased concerns over money laundering and the use of the global banking system to finance terrorist activities.

Under these new regulations banks are more accountable for detecting and preventing money laundering. This has pushed them to develop new processes and systems, hire extra compliance staff, closely monitor transaction activity through accounts, and report any suspicious activity detected. However, as banks struggle to keep up with new regulations and implement procedural and technical changes to support them, there has been an unintended impact on the banking customer who struggles to understand information requests and comply with account opening and maintenance requirements.

As these impacts on the customer mount, and the costs to become compliant increase for banks, greater pressure is being placed on banks to develop solutions that will facilitate detection of money laundering. Developing a quick solution is however, a significant challenge for the banking industry.

2. IT ALL STARTS WITH DUE DILIGENCE

Know Your Customer (KYC) is a process whereby a financial institution verifies the identity of an account holder and understands the purpose of the account, otherwise known as performing Customer Due Diligence (CDD).

CDD first became formalized under the "40 recommendations" issued in 1990 by the Financial Action Task Force (FATF), where guiding principles on how to conduct CDD were defined for banking regulators around the world. In 2001, in response to weaknesses in how banks were implementing KYC processes to support customer due diligence, the Basel Committee published "Customer due diligence for banks," which aimed to strengthen this critical component of anti-money laundering and counter-terrorist financing.

Regulators responded to both the FATF recommendations and the Basel Committee with guidelines and regulations of their own. For example, the U.S. Patriot Act, which introduced the Customer Identification Program (CIP), aims to establish compliance standards for U.S. banks to follow when identifying the identity of an account holder. In simple terms, each bank must have a sufficient degree of certainty about the identity of the account holder and perform the necessary due diligence to verify that the information is true and correct. CIP programs now form the core of most AML regulations and KYC policies around the world, with each regulatory body enacting its own form of the guidelines.

The general requirements of CIP specify that financial institutions must collect documentation that prove the account holder's identity (such as a government issued identity card) in order to validate the exact name, nationality, and date of birth of the individual. This information is then used to ensure that the account holder has been clearly identified, and in the event of concerns raised over the use of the account, the bank will know exactly who to hold accountable.

Once documentation is provided by the customer to support the CIP requirements under the KYC process, and it has been evaluated for clarity, certainty, and risk, the bank should have a clear understanding of the customer's identity. Should any risk items have been flagged during the account opening, the KYC process would prevent the account opening from proceeding until safeguards had been put in place to mitigate the risk, or possibly even prevent the account from being opened in the first place.

On simple review, the information that is captured by a KYC program to satisfy CIP requirements should be easy for any customer to provide, and straightforward for any bank to collect and store. For example, government issued identity documents help to verify the identity of individuals, company registration certificates verify the formation of a company, board resolutions provide the necessary mandates for account opening, and organizational structures identify who has control and influence over account activities. These are all standard documents that any individual or company should have readily available to provide on demand.

Unfortunately, despite the simplicity of the request, there are underlying challenges that both the customer and the bank must overcome before the KYC process can be completed and the account be opened. What may appear to be a simple request on the surface can actually unearth many complexities that both the customer and the financial institution must resolve together.

3. THE NUANCES OF REGULATIONS COMPLICATE THE EFFORT

When taking a closer look at CIP requirements, there are significant nuances that challenge banks as they attempt to build KYC processes and procedures. In an effort to build a KYC framework that can accommodate each and every customer, the exceptions to the norm often derail the efforts to develop a simple process. As the bank attempts to build a single KYC process that accommodates a variety of customers, the process becomes increasingly convoluted and difficult to implement.

Take, for example, a simple requirement to present a document as proof of identity. This basic requirement immediately raises a myriad of questions and concerns for the bank. Is the bank required to be an expert in every government issued document worldwide? Is the bank responsible for ensuring that the document presented is valid? How does the bank know that the identity document is issued by a trustworthy body or official government agency? And if the customer is not physically present, how does the bank know that the document being presented is truly the individual opening the account?

These challenging questions get further complicated when the account beneficial owner does not have the documentation specified under the KYC requirement. For example, a U.S. citizen is not required by law to possess a government issued identity document, which is a standard requirement under KYC for many countries. If a U.S. citizen wants to prove identity and nationality, a birth certificate may be the only option available. However, if that individual has an account outside the U.S., a birth certificate may not be sufficient to satisfy local regulations, since it does not have a photo image of the individual. Again, the bank is placed in a difficult position of not knowing whether a legitimate document can be accepted as proof of identity, and the customer may truly have no other options to consider.

Lastly, customers may be very uncomfortable providing some forms of identity documents due to concerns over privacy. Government issued identity documents are generally accepted as means of proving identity, but in many countries they are seen as confidential documents. As the CIP requires that a certified true copy of the document be provided to the bank, the customer has the additional worry that the identity document copy is safeguarded against theft or intrusion.

4. THE ONLY CERTAINTY IS THAT ACCOUNT OPENING TAKES TIME

Unfortunately, the KYC process can quickly start to unravel as more nuances are discovered and the compliance more challenging. Decision-making to resolve the nuances takes time, as compliance officers are brought into the discussion and review to negotiate with business stakeholders. As the dialog evolves, especially around complicated situations where more risk is at stake, the customer must wait for a resolution.

"As the bank attempts to build a single KYC process that accommodates a variety of customers, the process becomes increasingly convoluted and difficult to implement."

This obviously impacts the customer, who needs to wait until the situation is resolved before the account can be opened. Not long ago, an account (even a business account) could be opened within two working days. Today, banks are reluctant to quote timelines to prospective customers because they know that the process could drag on for weeks and sometimes months.

Corporate clients are particularly susceptible to these delays in account openings, where there is often a genuine time sensitivity to a transaction that can impact the success of their business. These delays can have significant impact on a business, especially a new business that may be growing quickly and needs to process transactions in a timely manner to build trust with business partners.

And, it is not only the customer that is losing business, the bank itself is also losing revenue opportunities. The longer the client is left waiting for the account to be opened, the more expensive the account opening becomes and the greater the loss of revenue opportunity. Despite these losses, both sides are equally helpless and must endure the challenges together in the hope that the impact is not too great.

5. CUSTOMERS HAVE NO CHOICE BUT TO COMPLAIN

Many bank customers complain about the tedious process and sometimes invasive lines of questioning that accompany the KYC process. As the customer is driven through the KYC process, the mounting requirements seem impossible to fulfill and become obstacles in opening (or maintenance) of the account. Weeks, and even months, can pass by as issues encountered during the KYC process are escalated for resolution by a compliance manager who may be overwhelmed by the volume of questions or simply needs time to consider the situation.

If banking was an industry competing with other industries for the same market segment, they would fail simply due to customer dissatisfaction. From the outside, it appears that the banking industry holds its market hostage and is dragging its feet on how to become more customer service oriented with its KYC process. The only recourse a customer has is to complain and hope that their voice is heard over the others that are also voicing their frustration.

But, where does the fault lie, with the bank or the regulator? Both are probably to blame. The regulators have mandated KYC requirements that do not consider the variety of challenges faced in implementing them. Meanwhile, the banks have struggled to devise programs, build systems, and educate customer service teams in how to handle the variety of situations that can occur during the KYC process.

Needless to say, both banks and regulators have recognized these faults and are making efforts to improve the client experience.

6. THE DILEMMA FOR BANKS

To be fair, banks are aware of the negative impact that these requirements have on their customers and are very concerned about it. However, they are caught in a dilemma: should they take the time to develop a client friendly KYC process that will take considerable effort and resources to implement and manage, or risk customer satisfaction with a KYC process that is quick from a regulatory approval perspective but does not provide a satisfactory customer experience?

Many banks have been caught in the crosshairs of the regulators by not having a compliance department that is well versed in global regulations. Finding compliance experts who can review regulations quickly and effectively and translate them into meaningful policies and procedures is a daunting task. Particularly challenging is the fact that regulators have given short timelines with strict penalties if the regulations are not met.

The fear for any financial institution is that they will fail an inspection by a regulator and lose their license to operate. Loss of operating license, or any restrictions on the business, is a blow that can ruin any bank overnight and cause tremendous harm to account holders and their respective businesses. Regulators clearly want to avoid this outcome as much as banks, so there is often a period of time given to the bank to become compliant. However, in the scramble to make the necessary changes there is always impact on customers who struggle to fully understand and accept the changes that are not always well explained.

Further complicating the dilemma is that the bank needs to implement compliance standards that are “global” and cover each jurisdiction in which the bank operates. Designing a framework that is global, simple to implement and enforce, and do so in a way that makes sense and with minimal impact to customers has been the largest challenge for all banks. Most have often erred on the side of caution by implementing overly rigorous “global standards” programs that are challenging to develop with procedures that are difficult and confusing for internal staff and customers to follow. Unfortunately, a major consequence of not implementing the correct KYC compliance program, or one that is too weak, again is to receive another fine or potentially lose a banking operations license, which is far too great a risk to consider.

For certain, the intention of applying regulations on financial institutions is not to cause harm or difficultly for account holders. Although it is difficult for most account holders to see the mechanics of these programs, the complexity of a compliance program that is equally uniform yet bespoke to certain types of customers is not a realistic approach towards solving the problem. When a bank has tens of thousands, or even hundreds of thousands, of accounts that may be impacted, there is simply no way to evaluate each account holder on a case-by-case basis within a realistic time frame or resource pool.

7. HOW TO EASE THE COMPLIANCE STANDOFF

Most banking customers have a story or complaint to share about their experience with KYC. The level of frustration is significant, with both customers and bank staff who are perplexed and annoyed with the challenges of being compliant.

Banks are not good at change, but they are making an effort. And customers are not good at compliance, but they are slowly accepting it and making it part of their business planning. This does not mean that both sides need to be content with the current situation. Opening a bank account should not take weeks or months, and customers should have the right to use their accounts legitimately without undue scrutiny while issues encountered during the KYC process are resolved.

The easy – and often stated – solution to simplifying KYC is technology. This is a fair statement, but it overlooks genuine questions and problems. Yes, technology will enable a solution and be a key component towards its success. However, the true problem is the lack of common data standards and protocols, which if agreed – and not only across the banking industry but also between regulatory bodies – could trigger a banking compliance revolution.

Take again, for example, the issue with identity documents and the challenges that banks face in evaluating and accepting them. The purpose of the identity document is to validate the name of the account holder, their nationality, and date of birth. For the most part, the identity information that each bank around the world is collecting under a KYC program is much the same. From a customer's prospective, this information is static and, therefore, needs to be validated only once, so that it can be accepted whenever needed by any bank worldwide.

Under a global verification model, the customer completes the identification verification process only once with a trusted third party (which could be a bank or an independent company). Verified details are then certified by the trusted third party with a digital certificate that is then linked to the encrypted personal data file. Upon request, the customer authorizes the bank to access the encrypted file which is then validated through a key exchange that confirms the right to access and the authenticity of the data. Upon confirmation from the trusted third party, only the necessary personal identity details are transmitted from the data file to the bank, which then feeds them into the back office KYC system.

There are many advantages to this model, which in various forms is becoming known as "eKYC." The customer only needs to complete the identity verification process once and retains ownership and control over their personal details. The bank no longer needs to review and validate identity details, saving it tremendous costs and resources, as well as reducing risk of error. Most importantly, the process can be achieved in seconds, as opposed to the days or even weeks that it currently takes to obtain certified true copies of documents and have them accepted by bank staff.

This secure technology is already in use today and is widely available. The problem is how to agree on a common standard data format and which third party will be the trusted authority to verify and certify the identity details. Before any bank could accept such an eKYC model, it would need to be sure that the data format is consistent and that the regulators have accepted the third party as the independent certifier of the data. But, as we look at how common standard can be developed for an eKYC solution, we must look back at the fundamental CIP requirements and how KYC identifies individual account holders.

8. INTRODUCING EKYC AS A STARTING POINT

Many regulators are approving the development of eKYC solutions, although what exactly this entails can differ between countries. Certain locations in Asia, such as Singapore, Malaysia, and India already have regulatory approval for eKYC, but each is taking a slightly different approach with development. Although regulatory approval has been provided, how exactly eKYC is to be accomplished has not been specified, nor have the expectations surrounding the underlying technology.

EKYC simply means performing KYC electronically, or without paper (as is the current practice). For example, instead of asking the customer to present certified true copies of identity documents on paper (such as a passport), the bank can accept a digital identification card that can verify the individual through biometric scanning (such as a fingerprint). Personal details are linked to the identity card, either in a memory chip on the card or accessible through a secure online channel, which are transmitted to the bank to support

the customer's KYC profile. The customer then needs to only present the identity card at the time of account opening in order for the bank to receive the details it needs.

The time (and cost) difference of using eKYC solutions to identity individuals is substantial. Providing a certified true copy of an identity document can cost up to U.S.$100 per copy. When you consider that the document is sent by post, time becomes a considerable cost as well. However, an eKYC solution that leverages an electronic identity card accomplishes the identity verification instantly and has virtually no cost once the hardware and software have been installed. For customers, this is a major improvement over the current situation.

9. SAME CONCEPT, DIFFERENT COUNTRY

Leveraging electronic identity cards is, therefore, the logical starting point towards building a full eKYC solution. Conceptually, the electronic identity card is providing the same information about the individual as a standard government-issued document, such as a passport: name, date of birth, nationality, and possibly birth place and current residential address. However, even with those basic details in mind, every country is taking its own route with electronic identity cards.

In Malaysia, the MyKad identity card is carried by all Malaysia citizens. This identity card contains a chip that stores basic personal information such as name, date of birth, place or birth, residential address, and most importantly, a digital copy of a fingerprint along with a photo image of the individual embossed on the card. By combining the personal information along with the biometric validation, the MyKad can provide all required information under a customer identification program (CIP) to satisfy KYC requirements, which the customer simply needs to present at account opening.

In India, a program managed by the Unique Identification Authority of India (UIDAI) has been developed to issue a unique 12-digit identity number, called Aadhaar, to all individuals. Upon opening of a bank account, the customer provides their Aadhaar number and then authorizes the UIDAI to release personal details through either a single-use password or biometric verification. The bank account is then linked to the Aadhaar, which further allows the bank to receive the personal details and be immediately updated whenever there is a change.

In both examples, a unique identifier number has been assigned to the individual. It becomes a single point to which personal details are attached through an electronic storage mechanism. The difference between the two identity cards is around the technology used and the means of transmitting and verifying the data. Whereas the MyKad stores details on a memory chip embedded in the plastic card that can be verified by a fingerprint scan, the Aadhaar transmits details from a database held by the UIDAI and then verified through a password. Fundamentally, the data is the same but

the underlying technology is different enough to make them unique eKYC solutions. Yet, both are part of their respective countries' strategies in adopting an eKYC solution for their local banking industries, which are already proving to be a significant success in reducing time and costs associated with account opening and maintenance.

10. ADVANTAGE – LOCAL BANK

However, it is those technical differences in the approach towards electronic identity cards that make developing a universal eKYC solution so difficult. Despite the progress at the local level, solutions that are universal and span across borders are still out of reach. Consequently, the advantage is currently with the local banks that operate exclusively (or majority) in their home country. Because the local bank's resources are focused on the local market, they are at liberty to invest in an eKYC solution that meets their local regulator's needs. For example, a local bank in India can comfortably invest in the hardware to support the Aadhar knowing that it is a government-approved standard for India.

For the global bank, however, this is a problem. Global banks have systems and infrastructure that are shared across locations and are difficult to customize to local country requirements without incurring significant costs. Building applications and technology that are bespoke to one country is only undertaken when it is absolutely critical to the operations of the business in that location or mandated by local regulators. Otherwise, the underlying technology must remain consistent in order to minimize costs.

Although not impossible, building eKYC solutions that meet each country's unique approach towards identity verification will be costly and difficult to maintain if governments continue to adopt their own approaches. At best, global eKYC solutions are years away from deployment as countries continue to explore and standardize the underlying technology of their identity card system. In the meantime, many customers are discovering that holding an account with a large global bank does not mean better service when it comes to KYC. In fact, fulfilling KYC requirements with a large global bank, even on accounts held locally, is time consuming and costly and unlikely to improve any time soon.

11. TAKING REQUIREMENTS TO THE CORPORATE LEVEL

It is important to recall that KYC and CIP apply not only to individuals, but to corporate customers as well. As companies are also considered legal persons that can be account holders, identifying the company as both its controlling party and beneficial owner is also a requirement under any KYC program.

Banks are more challenged to perform KYC on companies due to the complexity of the corporate structure and the number of parties that need to be involved in the KYC process. However, some countries have simplified the KYC process for banks by making it a part of the company registration. The German Commercial Register (Handelsregister) offers not only the legal name and address of the company but also the current details about the controlling officers and their respective identification information (as required under law), which are required under KYC.

Banks in Germany only need to obtain the company profile details from the Handelsregister to have most of the details that are required for the KYC profile. Considering that both the government and the financial institutions have a need to know, it makes sense that both can leverage the same "golden source" of information. The only downside is that the electronic verification of company profiles through the Handelsregister is only accepted in Germany, and should that company have accounts outside of Germany it will need to follow a traditional paper-based process to provide the same details.

12. USING BLOCKCHAIN TO UNBLOCK THE PATHWAY

In Thailand, the Ministry of Digital Affairs has recently signed a memorandum of understanding (MoU) with a digital firm to explore the use of Etherium blockchain technology to provide its citizens with a national digital ID. How exactly the blockchain technology will be applied to a national ID system in Thailand has yet to be announced, but it is a clear indicator that Thailand also intends to implement a secure system that will provide a unique identity number to each citizen. Again, similar to other countries in the Asian region, this technical approach lays the foundation for the development of an eKYC solution for Thailand.

There has been much discussion around the use of blockchain technology to facilitate KYC, and in many ways, it should be a part of the solution. To be clear, however, blockchain technology is used to build a historical record by documenting sequential events that are interlinked within the digital record. Each block of the digital record chain is a single event that is based (and dependent) on the block that preceded it. By examining the blocks in their sequential order, the historical record of the underlying subject (or object) can be clearly traced and audited.

Cryptocurrencies, such as Bitcoin and Etherium, have used blockchain to track the value of their currency by recording every transaction event within the lifecycle of the currency. Similarly, the entire financial history of an individual can be written into a blockchain that records each transaction as a historical event. From a banking perspective, this can be useful in helping to understand and analyze the customer and their financial position while ensuring that a truthful record can be consulted as needed. From a governmental perspective, personal details beyond name and date of birth can be recorded in a secure file that also records those changes. Use of blockchain will also help to ensure accuracy of the individual customer's data as they apply for banking services by providing a historical financial record that is reliable and can be leveraged immediately.

The other facet of blockchain technology is the "distributed ledger," which enables collaborative recording of the events into the blockchain. Distributed ledger means that the recording of blocks in the chain is shared between participants, thereby making the full blockchain history both recorded and accessible to everyone. Due to the distributed ledger approach, the blockchain record becomes a more comprehensive picture because it encompasses the recording of events from a variety of sources instead of just one.

Although there is significant value in having an accurate and comprehensive financial profile of the individual, we need to revert back to the immediate objective of KYC, which is to identify and verify the identity of the account holder. Blockchain provides a historical record, but does not verify the identity of the individual on its own. However, blockchain technology does serve the broader objectives of KYC, which is to understand the intended use of the bank account and whether it matches the historical profile of the individual or company. Consequently, it should be considered as part of an eKYC solution but not a solution on its own. Without identity verification, blockchain solutions for eKYC will not be effective. Meanwhile, leveraging blockchain technology to develop an eKYC solution in tandem with electronic identity cards is a logical step in reaching a target state KYC solution.

13. HARMONY MAY NOT BE PART OF THE MUSIC, YET

Unfortunately, time is costing the banks dearly with regards to supporting KYC requirements. The pressure to find quick-win eKYC solutions is immense, even if the target state solution has yet to be defined. However, eKYC is waiting on how each country will implement a national identity card system that is electronic and integrated with the local banking infrastructure.

From a banking industry perspective, there is a clear advantage in validating identity from a single golden source, such as a government body. Global banks are now faced with immense pressure to accommodate a variety of eKYC solutions to support different approaches adopted by governments. Unfortunately, the lack of harmonization in data formats, data sources, technical approach, and capture techniques is challenging global banks to develop underlying technologies to support them all.

Driving the issue further between global standards and local customization are the concerns of the customers themselves, who as citizens have rights to privacy protected by their governments. Each country has a different perspective on privacy, and what constitutes personal information protected under its laws. Estonia, for example, has taken a broad approach to capture a wide variety of personal information under a single e-residency program. Under this program, any person in the world has the opportunity to become an e-resident with a unique identification number that can used worldwide and applied to all types of personal details such as medical records and financial statements. In some countries such as the U.S., this would cause great concern over access to private information whereas in Estonia it is seen as helping people share personal details on a need-to-know basis.

Finding the right path through the privacy landscape is the fundamental challenge of a truly global eKYC solution. Each country will find its own direction that will satisfy its citizens. Unfortunately, that means a disharmonious approach that will continue to challenge banks to find common solutions. Blockchain may provide some relief here with its ability to provide masked data, but again it is not the first step and is still dependent on some form of nationality identification number.

14. CONCLUSION

The cost of KYC compliance has been exorbitant for banks, mainly due to the lack of technology to support the process and the need to follow paper-based processes to complete the work. Hiring compliance officers and analysts, building of new systems, and training staff have an annual price tag that is staggering, with costs reaching over hundreds of millions of dollars for the larger global banks. And this does not even consider the fines and penalties that banks must pay for being non-compliant. The cost for customers is also significant, but probably best measured in lost opportunity and frustration which could be argued as the greatest cost thus far.

Ours is a time of transition for the banking industry, so it should not be a surprise to anyone that these challenges exist. The important point is that all parties are doing what they can to simplify and comply with the laws of their host and other countries. KYC processes exist to protect everyone and stabilize the global banking infrastructure. A financial system where money laundering is rampant only leads to a society where everyone loses, so we can all agree that any regulation and effort to fight money laundering is paramount in the banking industry.

The unfortunate part of the story has been the slow adoption of tools to facilitate the KYC process. Regtech, as it has come to be known, is still in its early days, with technology companies small and large racing to bring tools to market but with no proven global solutions (as of yet), although there is proven success at the local level that can leverage electronic identity cards. Even though banks want to implement such tools on a broader scale, the lack of global standards is holding them back. However, once eKYC standards can be agreed by intergovernmental groups and country regulators, and a more uniform approach is adopted on how electronic identity cards are issued, the regtech market will be quick to deliver solutions and banks will be better equipped to implement them.

Meanwhile, banks are caught in the middle and waiting for standards to be developed and agreed not only between countries, but also within each country's legal system. Conceptually, we can see that eKYC will be a marriage between a national identity card system and blockchain technology. However, exactly which party is the holder of the privacy key in this equation, be it a government or a trusted third party, is fundamentally where the debate lies. Until that is resolved and standards are agreed, banks must wait before committing fully to any eKYC solution.

With an agreed set of standards, tools to support eKYC will find their way quickly into the marketplace. Ensuring that these tools comply with not only banking but also privacy laws will be critical in their success and adoption by customers. The technology already exists to build these tools, and many countries are already adopting them for their own citizens. Overcoming the standards obstacle will greatly simplify the KYC process. The central focus of banking can then shift away from the regulation that aims to protect the customer interest, back to customers themselves.

References

Basel Committee on Banking Supervision, 2001, “Customer due diligence for banks,” Bank for International Settlements, Basel

New Straits Times, 2017, “CIMB receives sandbox approval for paperless customer identification.”, November 23,

Financial Action Task Force, 2010, “FATF 40 recommendations,” FATF/OECD, Paris

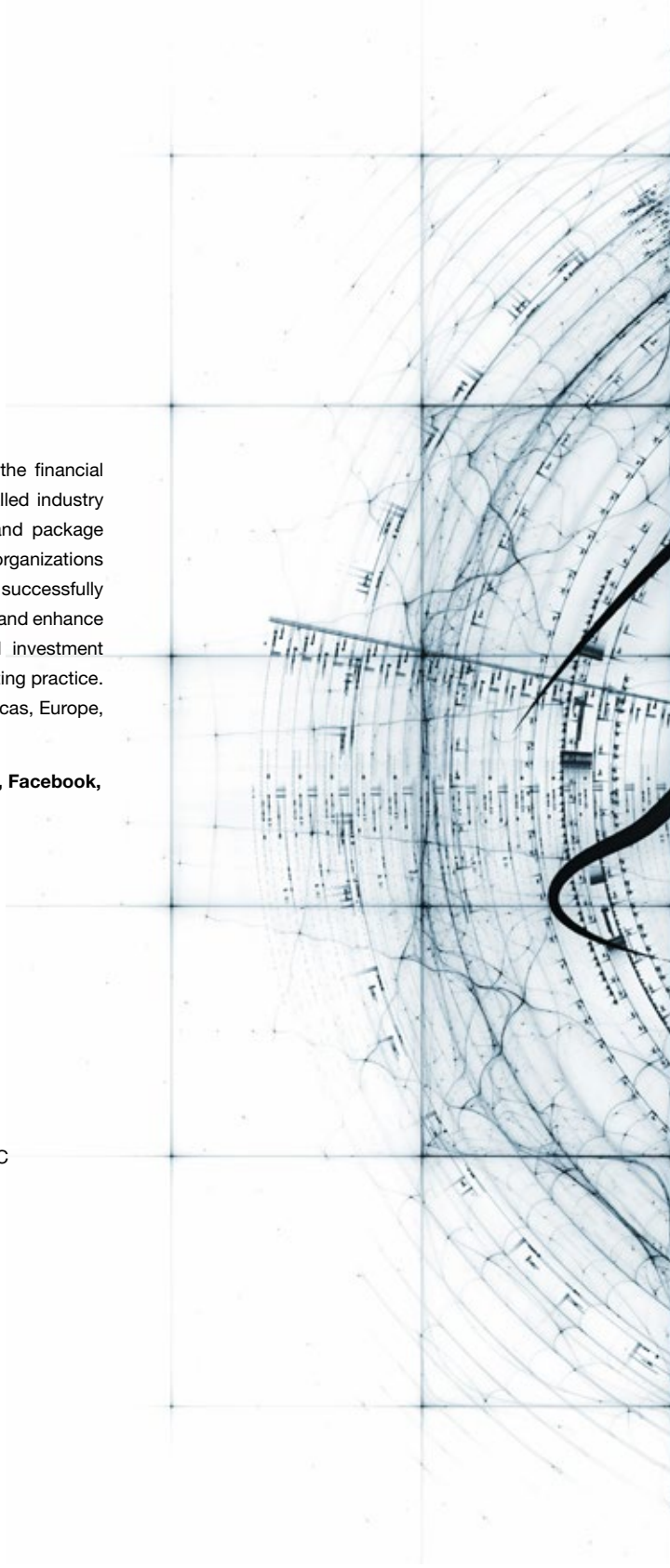
Financial Action Task Force, 2017, “International standards on combating money laundering and the financing of terrorism and proliferation,” FATF/OECD, Paris

Gupta, R., 2018, “Why biometric identification is required for KYC in digital India.” BW Businessworld. February 12

Heller, N., “Estonia, The Digital Republic.” The New Yorker. December 18 & 25, 2017

U.S. Department of Justice, 2001, “Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001,” Government Publishing Office, Washington D.C.

White, B., 2018, “Thailand mulls Ethereum blockchain for KYC program,” Bitcoin Journal, February 19



ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward. Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, and finance, risk & compliance. We also have an energy consulting practice. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Xing.**

WORLDWIDE OFFICES

Bangalore
Bangkok
Bratislava
Brussels
Charlotte
Chicago
Dallas
Dusseldorf
Edinburgh
Frankfurt
Geneva
Hong Kong
Houston
Kuala Lumpur
London
New York
Orlando
Paris
Pune
São Paulo
Singapore
Stockholm
Toronto
Vienna
Warsaw
Washington, DC
Zurich

CAPCO.COM

CAPCO