WHITE PAPER

Digital KYC and Today's World Post COVID-19

CODEBASE TECHNOLOGIES | Demystifying Digital Financial Services

Introduction

It is a generally acknowledged truth that, in times of crisis, one must be aware of the danger while also recognizing the inherent opportunities. The first quarter of 2020 saw the outbreak of the COVID-19 pandemic, which put the entire world to the severest test: how to face an unprecedented set of circumstances.

With the onset of the pandemic, the global financial world did not only see some industry trends accelerate, but also huge emphasis on hotly debated topics ranging from cash management, credit underwriting to digital transformation, cybersecurity, identity verification and customer data protection. Among them, the continuous need and importance in ensuring that the user is who they say they are when signing up for a product or service.

Historically, change has been the primary driver behind successful business worldwide, with precedence on technological innovation. In banking, the general perception towards change has been of acknowledgement rather than actual use and the traditional banking sector is a vivid example in this respect, with neobanks like N26 and Revolut tapping into banking services left outdated, such as payments and remittances.

While fintechs seemed to be better equipped for the COVID-19 situation, banks relying more on bank branches felt the negative impact as customers were required to stay indoors.

While fintechs seemed to be better equipped for the COVID-19 situation, banks relying more on bank branches felt the negative impact as customers were required to stay indoors. In the UK, for example, Lloyds Banking Group and Halifax decided to temporarily close a number of branches due to personnel shortages caused by self-isolation. In addition, some corporates that overlooked the booming digital environment registered negative figures by facing similar issues like the inability to access key data on customer preferences available only in the online environment. At the same time, other companies realized that measures relating to customer data management in a remote-only context had to be implemented in order to harvest valuable client data.

How to combine and analyze ever-growing volumes of data in order to get to know customers in the KYC process was a burning topic even before the pandemic. Once the outbreak turned to pandemic – with the situation thus creating a safe haven for fraudsters - having a clear strategy around how the security of customer accounts would be managed quickly became critically important.

55%

of businesses believe prospects might turn to competitors if their onboarding process takes too long.

Source: GLEIF research

Digital identity and **KYC**

The concept of digital identity is at the core of nearly every interaction of individuals, companies, and even devices, and it involves multiple distinct processes, such as determining what attributes can be used to identify a person, how to prove them over time, when to share them, and what a person can do with them.

In recent years, awareness and attitudes around customer identity verification has changed dramatically. Before the explosion of the digital economy, companies used to meet minimum identity verification standards not to enhance the customer experience, but rather to meet minimum due diligence requirements and avoid dealing with legal consequences. These anti-money laundering and KYC procedures have usually associated with high friction levels or bad customer experience.

The new digital economy brought about a significant change: financial services were too often implementing identity-checking processes that were not designed for the digital world. At the same time, customers were demanding a frictionless, timely, accurate and effective onboarding process. Thus, digital KYC has become a key component of the customer onboarding process to any financial service. Even more, apart from the financial services and banking sector, some new areas have emerged as a business opportunity for players providing digital customer verification: online education, gaming companies, crypto exchanges, to name just a few.

With eKYC, consumers are no longer required to go to the bank branch to open an account, thus making the onboarding process faster and more cost-effective. With the lockdown scenario triggered by the global emergency, eKYC has become the need of the hour for both SMEs and corporates.

However, there are challenges surrounding the adoption of digital onboarding solutions. For example, organizational culture may constitute an impediment, particularly in the case of those organizations where established processes are entrenched. Also, in an industry where many players haven't yet allocated the same level of compliance resources or regulatory expertise as others, fintechs can face a variety of challenges in setting up adequate eKYC processes. While traditional banking KYC requires customer physical presence for identification, the process is more laborious and with an additional level of risk when identifying the customer via online applications. In this regard, to supplement the lack of direct relation with the customer, fintech players bet on technologies like data analytics, AI and Cloud solutions to identify and emulate the customer profile automatically.

01 **Data Integration**

02 **Identity Verification**

03 **Validation (PEP & PFAC lists)**

04 **Real-time Risk Scoring**

05 **Ensuring Regulatory Compliance**

06 **Customer On-boarding**

What eKYC models are being used in different parts of the world?

The continuing transformation of local regulatory customer verification regimes to address digital and remote KYC was among the most important compliance topics, even before the crisis began.

On a national level, many regulators have already issued revisions or new guidance regarding remote customer verification to assist financial institutions in ensuring business continuity and compliant client onboarding during crisis situations. For instance, India's financial services market has a long history of KYC digitization by implementing Aadhaar. According to a McKinsey report, Aadhaar digital ID for eKYC was estimated to cut onboarding costs for financial institutions from about USD 5 (RM21.70) to just USD 0.70 per customer. Therefore, it comes as no surprise that even before the pandemic, The Reserve Bank of India amended the KYC norms (in January 2020), thus enabling banks and other lending institutions regulated by it to implement Video based Customer Identification Process (V-CIP). Only 3 months later, India-based Kotak Mahindra Bank was among the first lenders to allow video KYC. Similar initiatives were undertaken in other parts of the world, including:

- **Japan: in April 2020, Mizuho Bank announced a proof-of-concept trial of a new Digital ID in cooperation with Google Cloud Japan, Nomura Research Institute, and Dai Nippon Printing, supporting the online banking authentication process and ongoing CDD by utilising device location information and facial recognition technology;**
- **The Arab Monetary Fund announced during the same month the publication of Digital Identity and e-KYC Guidelines for the Arab Region issued by the Arab Regional Fintech Working Group;**
- **In May 2020, Citi expanded the reach of its CitiDirect BE digital onboarding platform, making it available in 37 countries and 5 languages;**
- **US-based Socure, a digital identity verification technology, launched 'Intelligent KYC' based on advanced graph analytics and machine learning.**

In a recent article published on Regulation Asia, Claus Christensen at Know Your Customer identifies four types of eKYC models, based on similarities and differences between existing schemes around the world:

The Swedish and Indian models: Digital ID Schemes

As mentioned previously, India is among the best examples to have in mind when it comes to eKYC systems, mainly due to its massive digital identity program called Aadhaar. While many industry voices refrain from confidently labeling it as a 'gold standard', Aadhaar is a great illustration of how a government-mandated digital scheme could work at scale.

Active since 2009, Aadhaar is now the largest biometric identification scheme in the world, counting 1.25 billion people registered as of February 2020. It's a unique, national 12-digit identification number that any registered entity can use to authenticate an Indian resident. The Aadhaar card serves as a proof of address and positive identification for a series of services and transactions in India, including opening bank accounts, obtaining a driver's license, filing income taxes, applying for social services or filing a death certificate.

In a similar move, in 2003 Sweden rolled out a federated BankID scheme, which was initially developed by a number of large banks. The eIDs created are now accepted as a form of identification also by government authorities, banks and organizations and the Swedish citizens can use their BankID for digital identification as well as signing transactions and documents for services ranging from online/ mobile banking, e-trade to tax declaration.

The German model: Video Check

During the pandemic, video KYC gained popularity as the next best alternative to face-to-face interaction. However, an interesting frontrunner in this area is Germany, whose regulator (BaFin) responded to industry demands for more convenient onboarding processes ever since 2014. At that time, BaFin published a directive which was updated three years later, thus enabling customer identification and verification via a live video call with a compliance department representative. Similar recommendations were made by the Reserve Bank of India (in January 2020) and the Monetary Authority of Singapore (in 2018).

The Hong Kong model: Identity Authentication & Matching

Instead of urging the industry to implement specific technologies, eKYC regulations under this model offer general guidance and remain open to interpretation and approve/reject specific procedures by financial institutions. A good example in this respect is Hong Kong. In February 2019, the Hong Kong Monetary Authority published an updated document on "remote on-boarding of individual customers", which does not include a specific checklist of actions to follow, but rather mentions identity authentication/verification and identity matching among the recommended technology for remote onboarding purposes. Malaysia and the overall European Union have adopted a similar approach, the same source reports.

The UK model: Enhanced vs Simplified Due Diligence

The Financial Conduct Authority in the UK is a particular case in the eKYC journey.

The Joint Money Laundering Steering Group (JMLSG) is the industry body which sets out comprehensive guidelines for practitioners to follow to comply with UK AML Legislation. According to JMLSG rules "for an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Roll) is not normally enough on its own to verify identity." (JMLSG Guidelines 2009 Section 5.3.38)

Thus, the standard level of confirmation, which is called 2+2, should include:

- One match on an individual's full name and current address, and
- A second match on an individual's full name and either her/his current address or his date of birth (JMLSG Guidelines 2009 Section 5.3.80)

The regulatory responsibility: from a stringent to a more Flexible approach

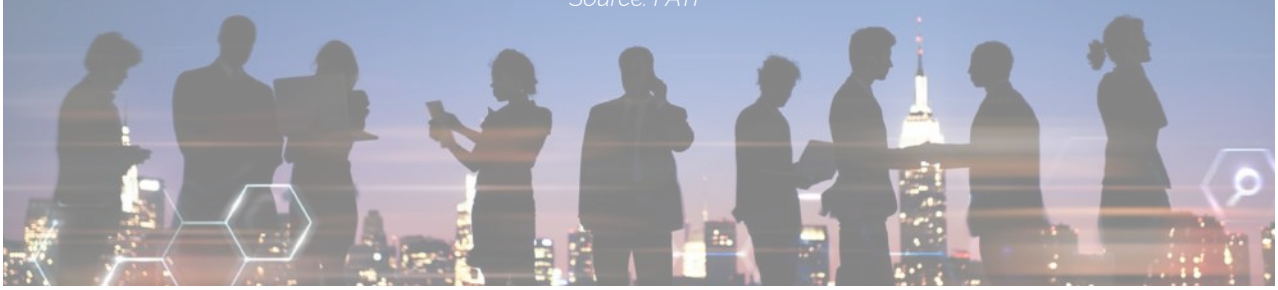
Discussions and attitudes towards the role and impact of regulation - or more specifically, whether legislation is a limiting or contributing factor to innovation - have dominated the industry for years. Inevitably, with the entire payments and fintech community immersed in such hot debates, the KYC-related aspects were no exception.

The constantly evolving regulations in every jurisdiction around the globe, coupled with a highly increasing growth of data (especially due to the COVID-19 crisis) have overwhelmed financial institutions with a series of challenges, especially related to digital data management. In order to design and implement the KYC process and strategy in particular, organizations had to address not only technological efforts/ aspects (which are considered complex and time-consuming, most often than not), but also regulations to be applied, as these must be carefully analyzed before implementing a new, digitalized approach. Such regulations, which establish the regulatory framework for digital KYC/AML processes, include: Anti Money Laundering/Counter Terrorism Financing (AML/CTF), the AML Directives and eIDAS Regulation in Europe, data protection and guidelines provided by local regulators (e.g. BaFin in Germany, CSSF in Luxembourg).

The burden brought about by the COVID crisis determined regulators to adopt a more lightened approach. Thus, more industry bodies were more understanding during the outbreak, therefore adapting KYC regulations or providing vital guidance on the benefits and risks of using digital identification methods during customer onboarding. To provide some examples: in March 2020, the Financial Action Task Force (FATF) released an official statement encouraging the fullest use of responsible digital customer onboarding.

"With people around the world facing confinement or strict social distancing measures, in-person banking and access to other financial services is difficult, and unnecessarily exposes people to the risk of infection. Use of digital/contactless payments and digital onboarding reduce the risk of spreading the virus. As such, the use of financial technology (Fintech) provides significant opportunities to manage some of the issues presented by COVID-19. In line with the FATF Standards, the FATF encourages the use of technology, including Fintech, Regtech and Suptech to the fullest extent possible."

Source: FATF



The announcement also references "the benefits of trustworthy digital identity for improving the security, privacy and convenience of identifying people remotely for both onboarding and conducting transactions while also mitigating ML/TF risks", as mentioned in FATF's Guidance on Digital ID, issued one month earlier.

Before the FATF published its official advice, various local regulators had already begun issuing revised guidance on remote customer identification. Among them:

1. **AUSTRAC, Australia's financial regulatory body, as well as the New Zealand regulator, adapted some of its KYC regulations for businesses during COVID-19, encouraging the use of e-KYC when possible and allowing organizations to verify customer identity with a digital copy of government-issued ID (such as a scan);**

2. **In a similar move, SEBI (Securities and Exchange Board of India) announced that foreign portfolio investors are allowed to provide scanned versions of the required documents upon registration;**

3. **The Central Bank of the Philippines temporarily lifted the requirement for the presentation of a valid ID card during client onboarding (only applicable if the amount of daily transactions does not surpass P50,000.00);**

4. **The Bangladesh Financial Intelligence Unit (BFIU) released new guidance and introduced eKYC for all financial services providers.**

Riding the digital wave in a **KYC-based** environment

Travel restrictions and social distancing rules during the pandemic forced businesses to conduct most of their work and client interaction remotely. This, however, required proper authentication and identity verification, and that fueled an increased interest in KYC solutions. With the accelerated adoption of digital technologies, the resulting userbase growth put the platforms to the test and increased the chances of vulnerabilities in the systems, which had an effect on customer security. And, inevitably, the following questions had to be addressed: what innovations can fintechs adopt to ensure client onboarding is swift, yet safe and effective?

Data Analytics

An important component of the KYC process is the authentication step, the first line of defence against potential fraud. It is also the first point of customer data analytics because they need to provide identification details like an account name and its associated password. Currently, there are two types of authentication, the two-factor vs three-factor authentication.

In the former case, a customer provides data on two aspects relating to something they have, something they own and something they know; in a typical case, when logging in to an online banking account the customer is required to insert a password (something they know) on their related smartphone or PC (something they have).

In the latter case, the customer is required to also provide the something they own component into the equation; in order to log in into their online banking accounts, for example, customers have to provide eye or fingerprint scans, among others. This is commonly known as the field of biometrics, a much more precise means of identification.

Many companies invest in research on improved biometric applications because it is foreseen as the future of secure authentication and a very lucrative industry. According to a study conducted by Biometrics Research Group Inc., biometric authentication market is expected to grow to USD 76.64 billion by 2025, from USD 17.28 billion in 2018, a notable increase. The same report suggests that this notable growth is being accelerated by the increasing use of mobile devices as biometric authentication tools; major smartphone manufacturers have already implemented facial and fingerprint scanners on their smartphones to swiftly and safely authenticate their users, while keeping theft and fraud at bay. Apple, for instance, uses a biometric authentication tool called Face ID whereby a customer is required to position their faces against the front camera for a full scan. The tool uses particular facial expressions and features as security elements during the phone unlocking process.

Furthermore, the main card systems VISA and MasterCard have introduced payment technologies using facial scans; MasterCard's solution is called 'selfie pay' and requires the user to have their smartphone scan the facial area easy authentication, thus eliminating passwords. Following this trend, some banks around the world like Citi and Chase have implemented biometric solutions like voice, fingerprint or facial recognition to make their users authenticate safer and faster. Voice ID, as well, has been in use, more specifically, in the bank call centres environments to enable rapid customer authentication. HSBC UK's Voice ID system identified no less than double the number of fraudulent calls in 2019 compared to 2018, a significant fraudproof ratio.

In the retail space, Amazon introduced the practice of palm waving in front of a palm scanner for easy customer identification. The customers have to previously link the palm, via smartphone, to a payment card so that the in-store scanner may accurately recognize the user, thus eliminating the need for smartphones or plastic.

In a bid to completely eliminate storefronts' physical cashiers, Amazon's GO platform solution has become available, as of 2020, to all the other retailers who want to pay for this biometric technology and customer data garnered by the American tech giant. The solution relies on in-store scanners analyzing the customers' facial and body features for a swift identification from the moment they enter in the shop. They need not scan a card or anything else to purchase what they need and just leave the store afterwards.

Artificial Intelligence (AI)

AI works hand in glove with data analytics because it draws all the needed information from it in order to keep fraud at bay. From the moment the customer logs in into their account, AI tools add every action into a private log or customer history to create behavioral patterns of that specific customer automatically. The richer the customer history, the more precise the tool is in correctly identifying the person who he or she claims it is. In Asia, for example, many banks have reached to the point where the customer boarding journey also involves scanning the customer's social media profile, besides the use of biometric solutions for a better digital customer profile. In this way, banks also tap into the customer's social behaviour element to combine it with the online banking activity for example and hence come up with a more complete customer profile.

AI solutions like IBM's Watson Studio work by monitoring every action made by a user and creating a specific algorithm meant to predict fraud rather than fighting it. If a sudden disruption in the typical user behaviour is spotted, then the system immediately investigates the issue and reports the 'anomaly'. If the user confirms the anomaly as part of their actions, then it is stored in the private history and turned into a rule for later cases. According to a recent survey, companies are already aware that AI is strengthening their ability to keep cybercrime at bay and that separate yearly budgets are dedicated to further expand research and use of improved solutions.

The Cloud

The previously mentioned IBM solution is also a good example of a cloud-based tool. The cloud is the place where the information is stored, typically a server that is communicating with another server and so on. Unlike a remote connection, which can easily become outdated, effective KYC tools need to constantly communicate with each other in a pattern we call platforms. Cloud solutions providers like Amazon AWS, Microsoft and Google offer effective fraudproof solutions for companies to work in a secure digital environment, by building improved authentication measures and safe storage solutions.

Platforms: a reliable KYC component

From a platform perspective, KYC processes can be safeguarded by government initiatives creating online databases where companies can look and check whether a customer is safe or potentially harmful.

In this respect, banks and financial services companies all over the world turn to publicly available centralized platforms like OFAC and EUR-Lex Sanctions screening platforms to ensure their KYC is performed adequately. These platforms gather data on all sanctioned individuals and entities that attempted to breach the financial laws of EU, US and other jurisdictions. The platforms can also be accessed via APIs for smooth integration and automation of the KYC process in real time.

In May 2020, the EU introduced the AML 5 framework whereby the member countries should develop a public UBO database in order for banks and financial services providers to consult and improve their KYC practices. This is a legal measure coming from regulators in an attempt to safeguard the financial system from potential Money Laundering and evasion. Similarly to the sanctions platforms, the soon to be created UBO register platforms will help businesses better identify their trade partner.

Based on the principle of working in the cloud, financial services companies started working with each other than against one another in a secure digital environment called open banking. The practice implies financial companies, like banks, to skip the silo perspective (competition) and embrace the information sharing alternative via Application Programming Interfaces (API) to the benefit of the participants. In this way, the bountiful information creates an added layer of security when identifying the customer because there can be created a customer traceability history, a digital alternative to Customer Due Diligence

Via APIs, participating banks can instantly exchange information about a customer's financial performance, for example, and eligibility for other banking services. Similarly, the participating financial companies can exchange ideas towards the bettering of the overall financial products instantaneously as a key word in working in this platform-based model is scalability. Such apps are designed to work for an array of situations and needs rather than for a constituent part, thus saving time, resources and improving security by non-stop monitoring.

As an example, corporates like VISA introduced platform solutions to help tackle online fraud like ID Intelligence which is aimed at both financial services providers and retail players in easing up their way to biometric solutions adoption. By adopting such platform solutions, via APIs, businesses can offer their customers safe and secure biometric-based authentication alternatives to shop, pay and perform banking services by only using their mobile devices.

Finally, open banking projects are leading the way forward with estimates projecting the industry at a valuation of USD 43.15 billion by 2026, with North America securing its first place during the period but immediately followed by Europe with a significant CAGR of 24% increase.

Conclusion

Long gone are the days when the typical transactional context implied a direct relation between business and customers. In the current digitally transformed transactional context business have to adapt and secure their products offerings in the online medium now more than ever. COVID-19 reminded us that we are experiencing a cultural shift towards digitalization along with its value-added propositions like convenience and innovation.

As well, businesses need to realize that a long-term enterprise relies on integrity and security measures as the foundation principles which need to be set in practice when applying the KYC procedures. These KYC procedures have suffered a tremendous shift in applicability from storefronts and bank branches to the digital medium. We have seen that an effective and up to date KYC solution relies on the following:

Data analytics; it is of utmost importance to tell who the real customer is and who is a potential fraudster by creating a customer friendly and secure authentication step.

Using AI-based monitoring tools; add an additional security level by using continuous monitoring of the customer behaviour to create prediction-based fraudproof solutions. After accepting a customer based on eligibility, financial services companies are required to continuously monitor the customer portfolio until agreement termination to safeguard the financial market from money laundering and counter terrorism financing attempts.

Cloud; make sure your business is entirely functional in a highly secure and scalable digital environment.

Open bank scenarios: design applications that are primarily scalable in order to fit as many business needs as possible. These applications should be API-based for easy implementation into a partner's system and customer-centric for enhanced adoption rates.

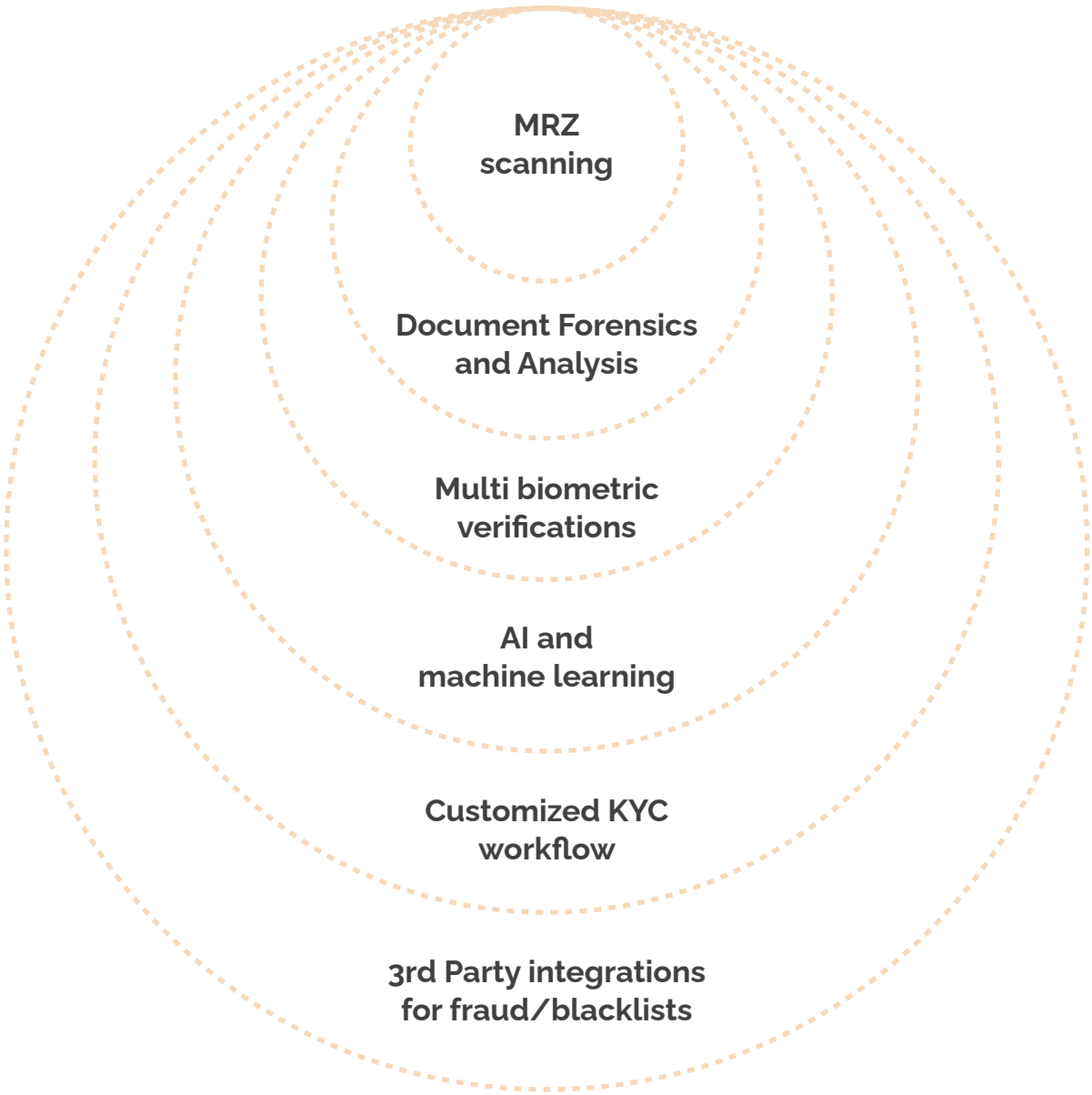
Create products designed for the digital context; create and design mobile-oriented applications as more and more customers migrate to this transactional context.

We at Codebase Technologies understand our partner and customer needs and, therefore, have created an impressive portfolio of Global Open API Banking solutions that enable banks and financial institutions to Demystify Digital Financial Services.

We help organizations create and deliver Innovative and Intuitive experiences across customer lifecycle. Codebase Technologies, with its award-winning suite of products, including the innovative Digibanc™, a comprehensive one-stop 'Bank in box', helps its customers unlock the true potential of the next generation of the digital financial eco-system.

eKYC process experts

Digibanc Identity, our cloud native and AI-powered digital KYC and compliance management platform, offers an integrated approach to KYC, AML and Compliance management boasting features like:



About Codebase Technologies

Codebase Technologies (CBT) is a Global Open API Banking solutions provider that enables banks and financial institutions (both Conventional and Islamic) as well as the emerging FinTech ecosystem to Demystify Digital Financial Services. We help organizations create and deliver Innovative and Intuitive experiences across the customer lifecycle.

With presence and customers across 4 continents, Codebase Technologies with its award-winning suite of products, including the innovative Digibanc™, a comprehensive one-stop 'Bank in box', helps its customers unlock the true potential of the next generation of the digital financial eco-system.

Get in touch with our digital banking specialists today to help you accelerate your digital banking journey.

Visit us at **www.codebtech.com** or get in touch at **marketing@codebtech.com**.

CODEBASE TECHNOLOGIES | Demystifying Digital Financial Services