Legal Aspects on the Use of AI in Digital Identity and Authentication in banks, its Impact on the Digital Payment Process

A research for investigating the Adaptation of Open Banking Concepts in Egypt

By

By: Dr. Sherif Mohsen Abdelfattah Shaltout

Abstract

Digital identification and authentication have become critical components in assuring secure and efficient digital payment processes as a result of the rapid growth of digital technology. This study explores the legal issues regarding the incorporation of artificial intelligence (“AI”) in digital identity and authentication systems, as well as the profound consequences for the Arab digital payment ecosystem. This document recognizes the growing importance of electronic Know Your Customer (eKYC) procedures as well as the general acceptance of digital identity in the banking industry.

People's interactions with online services and participation in digital transactions are being shaped by the fast-changing landscape of digital identity and authentication. This paper examines important conclusions, legal issues, and regulatory frameworks related to digital identity and authentication, with particular emphasis on the Egyptian banking sector. It looks at how regulatory organizations like the Central Bank of Egypt (“CBE”) and the Financial Regulatory Authority (“FRA”) might help provide safe online financial services. It is investigated if the emergence of regulatory sandboxes may promote financial innovation while maintaining compliance. To highlight the complexity of the regulatory setting, legal issues comprising identity verification difficulties, child onboarding regulations, the influence of legal capacity on digital identification, and consent management best practices are also explored. The eIDAS rule and the digital identification guidelines from NIST are offered as insights. The report ends by making suggestions for Egypt, such as boosting consent management, strengthening regulatory frameworks, encouraging collaboration, and implementing a national digital identity policy. While addressing legal issues and assuring data privacy, these actions work together to build a secure, user-centric, and innovative digital identity ecosystem.

Table of abbreviations

AI	artificial intelligence.
AAL	Authenticator Assurance Level.
AML	Anti-Money Laundry
APIs	Application Programming Interfaces.
AVMSD	Audiovisual Media Services Directive.
CCPA	California Consumer Privacy Act.
CBE	Central Bank of Egypt.
CMPs	Consent Management Platforms.
CSP	Credential Service Provider.
CTF	Combating the Terrorism Financing
DSA	Digital Services Act.
eIDAS	Electronic Identification, Authentication, and Trust Services.
eKYC	Electronic Know your customer
EU	European Union.
٢FA	Two-factor authentication.
GDPR	General Data Protection Regulation.
IAL	Identity Assurance Level.
IoT	Internet of Things.
KYC	Know Your Customer.
LP	Limited partnerships.
NER	Named entity recognition.
OCR	Optical character Recognition
OTP	One Time Password
RegTech	Regulatory Technology
RMF	Risk Management Framework
RP	Relying Party
SSI	self-sovereign identity
PIA	Privacy Impact Assesment
PSD٢	The second EU Payment Services Directive.

١. Introduction:

The Arab world is currently experiencing a digital revolution that has permeated various aspects of daily life, including the banking and financial sector. With the rising adoption of digital technologies, governments and businesses in the region have recognized the transformative potential of digital transformation in driving economic growth, enhancing financial inclusion, and improving overall efficiency (Al-Braizat, ٢٠٢٠; World Bank, ٢٠٢١).

١,١ Digital Identity Background and Context:

The world comprises a diverse range of cultures, languages, and economies, encompassing countries across the Middle East and North Africa. In recent years, the international trade and services have witnessed significant socio-economic changes, with an increasing emphasis on digitalization and technology integration across various sectors. Governments and financial institutions are increasingly leveraging digital tools to expand financial services and promote financial inclusion (Hoekman, ٢٠٢١).

In today's interconnected world, digital identity is about facilitating secure and convenient interactions while protecting personal data and preserving privacy. It encompasses technology, law, security, ethics, and user experience. Relevant in the context of digital identity are many factors and concepts: Authentication is the procedure of verifying a person's claimed identity. It entails supplying credentials (such as passwords, biometric data, or security identifiers) that are compared to stored records in order to grant access. After authentication, authorization determines which actions or resources a user is permitted to perform or access. This is essential for preserving security and privacy. Unique biological or behavioral characteristics, such as fingerprints, facial features, or vocal patterns, that can be used for highly secure and individualized authentication. The new trend is the concept of granting individuals control over their own digital identity, thereby reducing dependence on centralized authorities and enhancing privacy (European Commision , ٢٠٢٠).

The widespread acceptance of digital identity as a reliable means of identification has facilitated secure and efficient financial transactions. Digital identity enables individuals to authenticate their access to online banking services, conduct digital payments, and engage in various financial activities with confidence (International Monetary Fund, ٢٠٢٠). This increased trust in digital identity has catalyzed the growth of the digital payment ecosystem in the Arab world (World Economic Forum, ٢٠٢١).

١,٢ The Importance of eKYC and Digital Identity in Banking:

There are eight significant advantages to using eKYC in the digital onboarding process for banks (Jason E., ٢٠٢٠). First: eKYC is a fully automated web service that transfers Know Your Customer (KYC) data in real-time without the need for manual interaction. In contrast to paper-based KYC, which can take days or weeks, eKYC verification and issuance take only a few minutes. Second: Failed Acquisitions are Reduced: Digital onboarding is critical for gaining and maintaining clients. The digital method aids in lowering dissatisfaction and attrition rates caused by repetitive data entry and information verification delays. Third: Reduced Fraud: Banks have historically suffered revenue losses as a result of fraudulent operations, particularly with the introduction of digital banking. eKYC uses advanced technologies like OCR, facial recognition, and fraud detection to continuously monitor and authenticate users, improving security and minimizing fraud. Fourth: Improved Customer Experience: Onboarding reflects a bank's customer experience. Higher engagement results from eKYC's assistance in streamlining onboarding, which also boosts satisfaction and encourages more applications. Fifth: eKYC removes the requirement for physical branch visits by offering remote identity verification via biometrics and video conferencing. Customers and banks benefit from faster onboarding and enhanced convenience. Sixth: Competitiveness and Innovation: Innovations in eKYC processes, such as regulation changes and electronic document usage, present banks as forward-thinking and inventive organizations, offering them a competitive advantage. Seventh: Sustainability and document management: By removing the need for paper documents, eKYC's paperless approach decreases the carbon footprint. This not only helps the environment, but it also improves security and lowers the expenses associated with traditional document storage. Eighth: Integrating eKYC into company procedures boosts staff productivity and operational effectiveness dramatically. The streamlined method enables bank employees to provide efficient and accurate customer service.

Finally, implementing eKYC software enables banks to provide a smooth and safe digital onboarding experience. This not only attracts and maintains customers, but it also improves operational efficiency and increases the bank's market position.

١,٣ Legal Capacity's Importance in Digital Transactions:

Legal capacity in the digital world refers to an individual's ability to enter into legally binding agreements and conduct transactions. It is critical to ensure that people who conduct digital transactions have the legal authority to do so. This is necessary for numerous reasons First: Contract Enforceability: For a digital contract to be valid and enforceable, all parties involved must be of legal age. If someone lacks legal capacity, the contract may be challenged or declared null and void (Chamberlains, ٢٠٢٣). Second: Consumer Protection: Ensuring that persons have the legal capacity to grasp the terms and implications of a digital transaction protects consumers from entering into agreements that they may not completely understand. Third: Maintaining legal capability in digital transactions fosters trust and confidence in the digital banking ecosystem. People must have confidence that their rights and interests are being respected (Deloitte, ٢٠٢٢). Fourth: Ethical Considerations: The incorporation of artificial intelligence and other advanced technology into digital commerce poses ethical concerns. It is critical to ensure that individuals provide informed consent and understand the consequences of their actions (Frontiers, ٢٠٢٢). Fifth legal competence is taken into account in the design and implementation of these technologies. Legal competence is much more important in the context of digital identification and authentication. As artificial intelligence (AI) is increasingly utilized to facilitate these processes, it is critical to guarantee that persons' rights are protected (OECD, ٢٠٢١).

٢. Legal Aspects Regarding Digital Identity and Authentication:

Insurance of the security, legality, and trustworthiness of digital identity and authentication processes has become a major problem in the rapidly evolving ecosystem of digital transactions and online services. This section examines significant legal concerns that occur in the field of digital identity and authentication, offering insight into the challenges, potential hazards, and legal capacity implications.

٢,١ Identity Verification and Authentication Challenges:

To prove user authenticity in online interactions, digital identity verification and authentication are essential. The challenge of guaranteeing the accuracy and reliability of these processes, nevertheless, is substantial. One of the most serious problems is the potential for identity theft and impersonation because, as more personal information is shared and retained online, malicious users may try to take advantage of system flaws. Liability, accountability, and data protection issues related to identity verification and authentication help to reduce the danger of insufficient security measures or inaccurate verification methods.

By implementing robust identity verified against identity theft and fraudulent activities. This involves verifying individuals' identities solutions, businesses can establish a strong sense of trust with their customers and safeguard using a range of methods, including document checks, biometric data, and address verification. These measures not only streamline the process of user onboarding and account opening but also maintain a high level of security. An essential aspect of this process is the validation of passport images to confirm the individual's identity. However, while identity verification solutions offer numerous benefits, they also present their own set of challenges. Staying up-to-date with ever-evolving digital identity verification techniques employed by fraudsters and striking the right balance between rigorous biometric checks and a seamless customer experience are complex tasks that businesses must navigate effectively. In today's interconnected world, where biometric recognition plays an increasingly vital role in identity verification, organizations must adopt reliable methods such as passport scanning and streamlined onboarding processes. These approaches ensure both convenience and security. By incorporating biometric recognition technology, organizations can significantly enhance their ability to accurately identify individuals and prevent fraudulent activities. Innovative solutions provide organizations with the means to streamline their identity verification procedures and elevate their overall security measures (faceonlive, ٢٠٢٣).

٢,٢ Legal Issues Concerning Child Onboarding:

The digital age has led to the integration of technology into various aspects of children's lives, including their interactions with financial services and online platforms. Child onboarding, which involves the enrollment of minors for various services, presents unique legal challenges. One central concern is obtaining proper consent from a minor's legal guardian.

The legal landscape surrounding child onboarding is complex, as it often involves compliance with age-specific regulations and international standards. Failure to adhere to these legal requirements could lead to unauthorized data processing, privacy violations, and even potential harm to minors. Ensuring that proper consent mechanisms are in place and that data protection laws are upheld is paramount to avoid legal repercussions.

In April ٢٠٢٢, the European Parliament and member states reached a political agreement on the EU's Digital Services Act (DSA), which is expected to be adopted in January ٢٠٢٤. The DSA aims to harmonize regulations for controlling online platforms and addressing harmful and illegal content. As part of this initiative, the European Commission plans to establish a comprehensive EU code of conduct on age-appropriate design, building on the DSA rules and in alignment with the Audiovisual Media Services Directive (AVMSD) and GDPR. This code seeks to ensure the privacy, safety, and security of children using digital products and services. Collaboration between industry, policymakers, civil society, and children will drive this effort (biometricupdate, ٢٠٢٢).

The European Commission intends to support age verification methods that uphold privacy and security while being recognized EU-wide. Collaboration with Member States, stakeholders, and standardization organizations will strengthen effective age verification methods, promoting market solutions through a framework of certification and interoperability. The legislative developments reflect a growing trend toward requiring age verification solutions. Some Companies are actively monitoring global legislative changes and developing regulatory technology (regtech) solutions to meet emerging regulations. This approach offers a diverse range of age assurance options for organizations and consumers. The availability of operational solutions and the development of international standards for age assurance contribute to a healthy ecosystem of age verification methods (biometricupdate, ٢٠٢٢).

٢,٣ Legal Capacity's Impact on Digital Identification:

The legal concerns surrounding digital identification and authentication are complex and must be carefully considered to assure the security, legality, and fairness of digital interactions. Identity verification issues, child onboarding rules, and the impact of legal capacity on digital identity all contribute to the growing legal landscape in the field of digital commerce. Legal capacity, or an individual's ability to enter into legally binding agreements and transactions, is a critical notion in the context of digital identity. Digital transactions may be ruled void or unenforceable in the absence of proper legal competence. The incorporation of artificial intelligence (“AI”) and other modern technology raises the importance of legal capacity considerations even more.

The online environment, sometimes known as cyberspace, has particular characteristics that influence identity formation. Because of the abstract nature of the online environment, virtual acts may have different effects and moral judgements than real-world actions. Internet users act differently and shape their identities in ways that differ from those observed in the actual world. According to George Herbert Mead's Social Self Theory, people form their identities through social interactions, observations of others, and internalization of external thoughts and feelings. These exchanges take on new shapes in cyberspace (Ewa Michalkiewicz-Kadziela, ٢٠٢٢):

The evolution of digital tools and platforms has ushered in a new era of social connections, providing individuals with greater latitude to express themselves. Consequently, people utilize search engines and social profiles not only for observation but also for cultivating and enhancing their online personas. As a result, the digital environment has an impact on human identity creation, distinguishing it from real-world identity. Cyberspace provides the illusion of content supervision, allowing users to build separate identities, particularly on platforms where anonymity is prominent, such as social media. This is in contrast to systems that require real-time identifying data. Differences in online identity creation are influenced by a sense of freedom and new technologies. Given the internet's impact on identity, it is argued that digital human identity is distinct enough to justify additional investigation. This invites investigation into the distinctions between digital and real-world identities, recognizing the distinct characteristics that constitute each form (Ewa Michalkiewicz-Kadziela, ٢٠٢٢).

٢,٤ Consent Management best practices:

The General Data Protection Regulation (“GDPR”) is based on the "opt-in" principle, which requires explicit user consent for the processing of personal data. GDPR outlines a variety of legal grounds for processing, including consent, legitimate interests, vital interests, contract execution, public interests, and legal obligations. Consent must be given voluntarily, with knowledge, be specific, and be unambiguous. Infractions may result in penalties. Users should be able to withdraw assent without difficulty. Consent is required for non-essential cookies, such as Google Analytics and social media modules, and consent management requires the collection and recording of consent. Contrarily, the California Consumer Privacy Act (“CCPA”) does not require explicit consent for cookies, but it does require the display of privacy notices to users. The consent of a parent or guardian is required to collect information about minors (Secure Privacy , ٢٠٢٣).

Consent management entails the collection and documentation of consent. It includes collecting consent and maintaining consent records by regulations. Consent can be collected using custom banners, free solutions (which are frequently non-compliant), or Consent Management Platforms (CMPs), which automate the process and ensure compliance (Secure Privacy , ٢٠٢٣).

A cookie management platform is software that facilitates cookie consent compliance. It displays a banner that gives users the option to accept or decline cookies. It assists websites in complying with data protection laws in various countries. Best practices for consent management advocate the use of CMPs to outsource compliance to professionals, thereby ensuring conformance with privacy laws and user experience. User-friendly cookie banner designs are essential to establishing credibility where Secure Privacy provides a variety of banner designs to accommodate brand aesthetics and compliance needs (Secure Privacy , ٢٠٢٣).

Since the implementation of the General Data Protection Regulation in May ٢٠١٨, over ٦٠٪ of prominent European websites have requested visitors' consent for cookie usage. This has led to user fatigue regarding privacy notifications, driving the popularity of browser add-ons to suppress these banners. There's a growing call for a solution that streamlines consent across multiple websites or within browsers. A study made by Christine Utz and others focuses on analyzing the graphical user interface of consent notices and conducting three tests on a German website with ٨٠,٠٠٠ unique users and examines the impact of notice placement, choice types, and content framing on consent. Notably, messages displayed in the lower-left corner of the screen yield higher user interaction. When presented with a choice between tracking and other options, users tend to favor tracking over individual category or business approvals. The study also highlights the influential role of nudging in user decisions. It emphasizes that even seemingly minor implementation choices significantly affect user interaction with consent notices. Ultimately, the findings underscore the importance of regulations in ensuring users can make well-informed decisions by outlining specific rules or guidelines for obtaining consent (Utz, ٢٠١٩).

٢,٥ NIST digital identity Guidelines:

The digital identity architecture described in the NIST SP ٨٠٠-٦٣-٣ standards takes into account the products and services that are currently on the market (NIST, ٢٠٢٠). It recognizes the possibility of more complex models with several parties sharing functions. A person's real-world identification is verified once they sign up for a subscription after completing the proofreading process, according to the standards, which describe a digital identity as a distinct representation of a participant in online activities.

According to the recommendations, the IAL (Identity Assurance Level) is a common indicator of how well identity verification works. While IAL٢ and IAL٣ require attribute verification, IAL١ only requires self-declaration of attributes. The entity requesting authentication is known as the Claimant, and the verifier confirms their identity.

By using a mechanism to show ownership of authenticators to a verifier, authentication is defined as fostering confidence in the claimant's identity. AAL (Authenticator Assurance Level), in contrast, gauges the efficiency of authentication. Single-factor authentication is required by

AAL١, two-factor authentication is required by AAL٢, and a hardware-based authenticator that resists impersonation is required by AAL٣ (NIST, ٢٠٢٠).

The use of pseudonymous identities is permitted under these rules, which also provide a way to increase privacy by decoupling proofing from authentication strength. Authentication affects authorization decisions, and an RP (Relying Party) may transfer identity functions to a CSP (Credential Service Provider). The rules do not forbid RPs from asking for post-authentication data. The standards place emphasis on the value of informed consent, identity strength, and privacy considerations in managing digital identities and authentication procedures. Additionally, they offer normative backing for publications relevant to the NIST Risk Management Framework (RMF). They support the implementation of digital identity-specific risk management procedures within the RMF lifecycle stages.

In order to provide effective identity services, these guidelines advise assessing the risks and impacts of each component separately rather than integrating verification, authentication, and federation requirements into a single strategy.

The Key details of this guidelines are as follows (NIST, ٢٠١٧):

Focus of risk assessment: To reduce security and privacy risks, emphasis is placed on fixing potential flaws in identity verification, authentication, and federation.

Independent evaluation of the risks associated with errors in verification, authentication, and federation to establish the level of confidence for each transaction. Introduction of effect categories specific to digital identification that will help firms make wise risk management choices.

Risk-Driven Decisions: It is encouraged that while making technology-related decisions, security and risk management be given precedence over technological trends.

Acceptance Statement for Digital Identifiers: Once risk assessments are finished, agencies are required to develop a "Digital Identity Acceptance Statement" to make sure that they are in compliance with security guidelines and risk management techniques.

Utilizing IALs (Identity Assurance Levels) enables companies to ascertain the level of assurance necessary for allowing access to resources or services by evaluating the effectiveness of identity proofing and verification measures.

AAL (Authenticator Assurance Level): A measure of the effectiveness of the authentication process and the relationship between an authenticator and a person's identifier.

The choice of assurance levels and technologies for identity verification, authentication, and federation should be made using a risk-based process. The objective is to reduce flaws in each component to produce a more effective and secure method of managing digital identities. Given the range of authenticator types and increasing concerns like weariness and interception assaults, there is a need for more precise guidelines on determining assurance levels. Government and business organizations are working to apply the NIST Digital Identity Risk Management guidelines and provide supplemental materials. But both the assessment of assurance levels and current authentication have a need for more thorough instruction.

٢,٦ eIDAS regulation:

The acronym eIDAS stands for "Electronic Identification, Authentication, and Trust Services." In order to establish a uniform framework for electronic identity, electronic signatures, electronic seals, electronic documents, and other electronic trust services among EU member states, a European Union (EU) legislation was developed. The eIDAS Regulation is essential for the security of cross-border transactions because it enables trustworthy electronic interactions. It permits individuals to access online services in other EU countries using their national electronic identification schemes (eIDs). This regulation establishes a European market for trust services and accords them the same legal standing as their traditional paper-based counterparts. An evaluation of the eIDAS framework was conducted, including stakeholder consultation, surveys, and interviews, to ensure its efficacy and compatibility with technological and legal advancements. This regulatory framework seeks to ensure the legal validity of digital services, thereby encouraging businesses and citizens to adopt digital interactions naturally (European Commision , ٢٠٢٠).

For banks, customer onboarding and new account opening are complex and time-consuming processes, involving numerous checks like KYC, AML, and CTF. These checks extend to corporate clients, including key personnel and shareholders. Each stage requires extensive document verification, and mistakes can lead to regulatory issues or customer loss. The eIDAS regulation is welcomed by banks as it provides a standardized electronic identification system across the EU. These speeds up account opening and KYC updates, reducing compliance costs. With a pan-European eID framework, banks can tap into customers from other EU countries, compete in the Single Market, and potentially pass on cost savings to consumers, creating a beneficial scenario for all parties (cryptomathic, ٢٠٢٢).

٣. The Impact of AI on the Digital identity Processes in banks:

While artificial intelligence (AI) has greatly improved institutional digital identity processes, it also poses issues with data privacy, potential bias in algorithms, and AI model security. The right balance between innovation, security, and ethical considerations is essential as banks continue to deploy AI-driven solutions for their digital identity operations. While artificial intelligence (AI) has greatly improved institutional digital identity processes, it also poses issues with data privacy, potential bias in algorithms, and AI model security. The right balance between innovation, security, and ethical considerations is essential as banks continue to deploy AI-driven solutions for their digital identity operations. As a result, AI has significantly changed how banks handle digital identification, revolutionizing the way they verify customers, stop fraud, and enhance security in general.

٣,١ Using AI to Improve the eKYC Process:

The know your customer (KYC) process requires automation because without it, there will be more human errors, the time required to complete the KYC process will be longer, and the COVID-١٩ outbreak has reduced human-to-human interaction, thus automation would be good. ID and document verification are part of the KYC procedure. Financial institutions, such as banks, must undertake KYC in order to serve consumers. It can take up to ٣-٥ business days to validate the documents while performing online KYC. The system seeks to solve this problem by applying AI to automate this time-consuming task. To automate the widespread E-KYC procedure, the suggested solution makes use of AI and deep learning. The system reads the first and last name, and date of birth, recognizes it, and gives information that the client can directly use (Springer, ٢٠٢٢).

Existing KYC implementation techniques include human contact and data entry, which leads to inaccuracies in forms filled out manually on paper, difficulties reading handwriting, and probable errors during data entry by authorities. Even secure methods of authentication, such as OTP, can have data entry problems. Personal biometrics necessitate government officials verifying them at one's house, necessitating the individual's presence. To address these issues, an AI and deep learning-based system is proposed for automating the E-KYC process. The technology extracts and displays vital information for direct usage by the user (Springer, ٢٠٢٢).

The procedure could involve image enhancement, which involves editing uploaded document pictures. By utilizing median filters to reduce noise, noise reduction increases readability. Since the system uses an AI object detection model to determine the type of document, the next stage is the extraction and detection of features as a refinement. Feature extraction, which also trains a deep learning model, determines the format of the paper. Afterward, use text extraction and recognition. OCR extracts and verifies data from pictures that have been subjected to text extraction. From OCR output, custom named entity recognition (NER) pulls important data. The proposed AI-driven approach aims to streamline E-KYC by automating the extraction and validation of crucial data. By eliminating the manual mistakes that were prevalent in earlier KYC methods, this solution improves the accuracy and efficiency of the procedure (Springer, ٢٠٢٢).

The artificial intelligence-based optical character recognition technology will be highly valuable because it eliminates the need for manual labor in the KYC process, speeds up the procedure, and makes it more efficient by eliminating the possibility of manual error. eKYC solutions would be a significant advance over the existing manual KYC systems, making it a viable alternative for any location that requires an E-KYC.

٣,٢ AI Bias and Fairness in Identity verification in banking:

Christina Catenacci refered to the socio-technical approach as a way of describing how people interact with technology in a larger social setting. while there are numerous approaches that seek to build AI responsibly, guidance from a wider socio-technical viewpoint is required in order to control the dangers of AI bias, operationalize values, and establish new standards for how AI is developed and used. She wants to offer a starting point for creating comprehensive socio-technical recommendations to recognize and handle AI bias. In special publication, the three types of bias in AI—computational, systemic, and human—are identified, described, and discussed, along with the three major obstacles to bias mitigation. she concluded by offering some initial advice and stating that NIST plans to carry on with this work and develop additional advice and standards in the future (Catenacci, ٢٠٢٢). However, there is a growing concern about bias and fairness in AI systems used in the financial industry and beyond. As models are designed and trained based on data, there the banking is a risk of inadvertently introducing bias or relying on proxies that do not accurately represent individual circumstances (Craggs, ٢٠٢٣).

AI can contribute to bias and unfairness in banking systems, its impact on the future of banking, and strategies for avoiding unintended consequences when leveraging technology for financial services as industry has been rapidly transformed by AI, which has provided innovative solutions for streamlining operations and improving the consumer experience. Consider chatbots enabled by artificial intelligence, which are used to interact with customers, guiding them through their financial concerns while assisting banks in reducing labor costs (Craggs, ٢٠٢٣).

In addition, machine learning algorithms play a crucial role in detecting fraudulent activities by analyzing massive quantities of data that would be impossible to manually manage. In addition to detecting fraud, AI models can assist banks in identifying potential risks during the loan approval process by evaluating applicants' creditworthiness based on a variety of criteria, including payment history and outstanding debts. Personalized recommendations are another application of AI. By leveraging customer data such as transaction history or online behavior patterns, banks can provide services and products that are customized to satisfy the needs and preferences of each customer (Craggs, ٢٠٢٣).

Racial bias and AI are intertwining more and more in the modern world, causing serious problems in our daily lives. Machine learning models that are biased can be identified by their exclusionary behaviors, such as the refusal of loans to certain groups, restrictions on technological accessibility, or inconsistent functionality. Bias hazards increase as AI becomes more commonplace in society.

Facial recognition is a good example of racial bias in AI, but it is not the only issue. Age, gender, socioeconomic level, and device quality are all demographic variables that can affect how well AI matches faces to databases. The effectiveness of the database itself is crucial to maintaining bias. Software for facial recognition uses biometrics to compare facial traits to a database, which could produce unreliable results. The American Civil Liberties Union (ACLU) looked closely at Amazon's Recognition face recognition technology in ٢٠١٨ and found that it had incorrectly matched ٢٨ members of the US Congress with criminal mugshot files. Notably, although they make up only ٢٠٪ of Congress, over ٤٠٪ of erroneous matches involved members of other races.Facial authentication, which differs from facial recognition, establishes a person's identity using distinctive biological traits. However, even in this field, machine learning-powered AI algorithms may display racial, age, and gender bias. This bias doesn't depend on database quality like facial recognition does because it doesn't conduct enough searches against well-known image databases. Growing cause for worry Interest in mitigating demographic bias in AI-driven identity verification solutions has increased recently. This rise in focus could be attributable to more public dialogue spurred by movements like Black Lives Matter that highlight different aspects of injustice (Jumio, ٢٠٢٠).

Therefore, the interaction between racial bias and AI presents a variety of problems that affect both facial recognition and facial authentication. It is essential to address these biases in AI algorithms to guarantee that everyone, regardless of their demographic traits, has fair and equitable access to technology and services.

٣،٣ AI-Powered Legal Compliance Strategies:

Artificial intelligence-powered legal compliance solutions provide considerable benefits in terms of efficiency, accuracy, and the ability to respond to changing legislation. Human oversight and legal knowledge, on the other hand, are still required to understand AI-generated insights and make strategic compliance decisions.

AI-powered legal compliance solutions use AI technologies and tools to improve conformity to legal regulations and standards. These solutions cover multiple industries and employ artificial intelligence algorithms, machine learning, natural language processing, and data analytics to monitor, analyze, and ensure compliance while decreasing human errors and operational hazards. There are number of AI areas that ensure legal compliance such as Regulatory Analysis and Compliance as AI monitors regulatory changes and industry standards on a continual basis, analyzing updates to anticipate their influence on organizational operations and enable proactive compliance adjustments. AI analyses possible compliance risks by analyzing historical data, transaction records, and context, forecasting areas of noncompliance, and guiding resource allocation.in addition, AI examines legal documents such as contracts and vendor agreements to ensure compliance with regulatory requirements and to reduce the risk of breaches and penalties. AI systems detect trends in transaction data as part of AML (Anti-Money Laundering) and Fraud Detection that indicate money laundering or fraud, hence improving financial institution compliance. Moreover, AI maintains personal data by tracking flows, identifying risks, and automating data subject requests, all while guaranteeing GDPR and data protection regulations compliance as part of GDPR Compliance and Data Protection. AI can analyze tips and complaints from whistleblower hotlines, discovering trends that may suggest violations of compliance. Furthermore, AI monitors transactions in real time, identifying variations from normal behavior that may indicate a violation of compliance. Artificial intelligence analyses audit trails to find irregularities in company operations, thereby reducing internal fraud and assuring transparency. Litigation and Regulatory Enforcement Predictions: Based on past data, AI forecasts the likelihood of lawsuit or regulatory measures, allowing for proactive planning.

These AI-powered solutions improve compliance operations' efficiency, accuracy, and adaptability, but human oversight and knowledge are still required for evaluating information and making strategic decisions.

٣,٤ GDPR and Customer Data in AI Identity Verification:

The use of client data for AI identity verification processes is governed by the General Data Protection Regulation. GDPR is a comprehensive data protection policy implemented by the European Union to protect individuals' rights and privacy when their personal data is processed. Organizations must follow GDPR requirements when deploying AI for identity verification to ensure the lawful and ethical management of customer data. Here's how GDPR, customer data, and AI identity verification intersect: organizations using AI for identity verification must negotiate GDPR principles and standards to ensure customer data is processed lawfully, transparently, and securely. Balancing the benefits of AI with privacy concerns is critical to establishing trust and adhering to regulatory regulations. GDPR mandates that organizations have a legal basis for processing personal data. Consent is a frequent basis for AI identity verification, although processing may also be required for contract fulfillment (e.g., delivering financial services) or compliance with legal duties. Purpose Limitation: Organizations must ensure that consumer data obtained for AI identity verification is only utilized for its intended purpose, which is identity verification. Any secondary uses must be informed fully and consented upon. Data Minimization: GDPR emphasizes gathering just the information required for the given purpose. AI identity verification should only collect necessary identity information to reduce the risk of data exposure. Data Accuracy is also critical in artificial intelligence identity verification. Organizations must ensure that the customer data they use for verification is correct and up to date. GDPR requires businesses to put in place sufficient security measures to protect customer data. Because AI identity verification involves sensitive personal data, comprehensive security measures are required to avoid breaches. The GDPR gives data subjects various rights, including the ability to access, rectify, erase, and limit the processing of personal data. Customers' rights must be exercised through means provided by organizations. Customers must be informed on how their data will be used, including the use of artificial intelligence for identity verification. Privacy policies should clarify the process, purpose, and legal basis in detail. If AI identity verification requires transmitting data beyond the EU, organizations must follow GDPR cross-border data transfer requirements, such as using GDPR-approved procedures such as Standard Contractual Clauses. GDPR specifies specific timeframes for personal data retention. Organizations should only keep consumer data for as long as necessary for verification and then destroy it. AI-powered identity verification may necessitate automated decisions. The GDPR requires organizations to explain such decisions, especially where they have legal or significant consequences for individuals. Before deploying complicated AI identity verification systems, a PIA can help identify and minimize any privacy problems. Organizations that use third-party AI identity verification services must ensure that these vendors comply with GDPR and use sufficient data protection practices (Martin Hasal, ٢٠٢١).

Arner et al. (٢٠٢٢) highlight the connection between PSD٢, GDPR, and eIDAS. GDPR protects personal data processing, granting control rights to individuals. This mirrors the open data concept of open banking. While GDPR is EU-focused, it has global impact, inspiring similar laws worldwide. eIDAS aims to harmonize digital identities within the EU, enhancing customer convenience and business onboarding while EU open banking is fragmented, the legal framework comprising PSD٢, GDPR, and eIDAS has laid a foundation for broader digital services regulation (Frei, ٢٠٢٣).

Video identification, also referred to as video KYC (Know Your Customer) or video verification, presents a swift, user-friendly, and notably secure approach to confirming the identity of customers online. The implementation of a robust video identification procedure establishes a formidable barrier against various forms of identity fraud. This method not only incorporates human assessment but also integrates AI and machine learning, thereby substantially lowering the likelihood of online fraud occurrences. Moreover, this process ensures the highest level of compliance adherence. By engaging in video identification, an organization can demonstrably show their commitment to meeting regulatory requirements and upholding the stringent standards set forth by compliance frameworks.

Authentication of user identity is not always required, especially when users seek help on websites. Authentication is necessary when the application handles user data, like in banking inquiries. This involves verifying valid login credentials, like username, biometrics, or passwords, to create secure authentication tokens for the user's session. These tokens are temporary and need periodic renewal. Enhanced data protection is achieved with two-factor authentication (٢FA), such as email and text verification. Multi-factor methods are rarer. Authorization ensures right access to data and services. Personal authentication security, like a "Personal Scan," could further confirm user identity during the interactions with the application, preventing misuse by malicious actors when sharing personal data online (Martin Hasal, ٢٠٢١).

٣,٥ Right of Data erasure in GDPR:

Article ١٧ of the GDPR establishes the Right to Erasure, which permits individuals to request the deletion of their personal data from data processors under certain conditions. This includes situations in which the data is no longer required, unlawfully processed, objected to by the data subject, assent is withdrawn without legal grounds, the data subject was a minor at the time of collection, or erasure is required by law. The data must be erased without delay, and controllers must notify individuals within a month, extendable to two months, and inform third parties processing the data of the request for erasure (Eduard Rupp, ٢٠٢٢).

Exceptions to data erasure include instances in which data processing is required for freedom of expression, legal obligations, public health interests, archival or research purposes, or legal claims. Article ١٧ compliance is one of the GDPR's challenges for businesses, with ٤٢٪ of respondents to a survey expressing concern about it. In addition, many businesses lacked a comprehensive comprehension of GDPR, and the process of erasing old data necessitated modifications to existing procedures. According to research, conformance with requests for data portability was not always met, and in some instances, the data was not in a compliant format. Past research indicates that app and website vendors comply with deletion requests to varying degrees, ranging from ٤٨٪ to ٥٧٪ after two requests (Eduard Rupp, ٢٠٢٢).

٣,٦ Rapid Development of Self Sovereign Identity (SSI):

Interoperable digital identity management is gaining significance because individuals possess multiple partial identities that pertain to various aspects of their lives. Each partial identity can contain overlapping or distinct information. It is essential to ensure the portability, interoperability, and user-controlled administration of these partial identities. The expansion of digital interactions presents challenges. It is not possible to directly translate physical identity management systems into the digital sphere. Digital identity management is comprised of distinct phases, each with its own characteristics and challenges: First: "Centralized Identification:" This method lacks user control and interoperability because it is managed by system-level entities. It is challenging to remove the identity, and users rely on the entity for identity management. Second: User-centric identity: Users control their access to services, but the use of multiple credentials poses security risks and is inconvenient. The respective providers store the attributes of fragmentary identities. Third: Federated Identity: Enables the exchange of partial identities across providers via a single sign-on instance. This method is highly dependent on the identity provider and raises concerns about monitoring and abuse (Jens Strüker, ٢٠٢١).

Existing identity management techniques have limitations, such as a lack of interoperability and reliance on particular parties. No widely deployed system addresses all of these issues and user requirements effectively. In the context of expanding digital interactions, the development of digital identity management endeavors to strike a balance between user control, security, and convenience. Verifiable credentials and decentralized ledger technologies have the ability to provide trustworthy digital identification solutions for all types of entities, including people, businesses, and organizations. This might result in reliable online interactions. The severe societal demands brought on by the present pandemic issue have further accelerated the technology's quick development, known as self-sovereign identity. To increase the acceptance of SSI, governments, non-profit organizations, businesses, and individuals are working together on various SSI-related projects (Laatikainen, ٢٠٢١).

Self-Sovereign Identity is a decentralized method of digital identification that grants ownership over digital identities to entities including people, organizations, and objects. It makes use of blockchain technology to improve security, reduce dependency on outside authorities, and address problems with conventional identity systems. User-centric and decentralized, SSI allows for the exchange of verifiable credentials directly between parties. User control, security, privacy, consent-based data sharing, data integrity, and trustworthiness are the major goals. The attributes of SSI are divided into three categories: security, controllability, and portability. Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, Minimization, and Protection are among Allen's ١٠ guiding principles. The Security, Controllability, and Portability components of these principles are organized with an emphasis on data security, user control, and identity portability. Decentralization, equity, usability, verifiability, and authenticity factors are added to the principles (Cucko, ٢٠٢١).

Self-Sovereign Identity is a novel concept shaping digital identity management. It advocates users' autonomy in creating and managing their identity without relying on centralized authorities. Decentralized Identifiers (DIDs), as defined in the W٣C specification, play a pivotal role in this approach. DIDs are user-controlled identifiers, divorced from centralized registries or identity providers, resolving to DID Documents containing proof purposes, verification methods, and service endpoints. While DIDs only identify, they are paired with Verifiable Claims (VC) for sharing user information with third parties, proving ownership of attributes through cryptographic links between VCs, DIDs, and issuers. Trust in the issuer can be established through various means. Users retain control over the information they share, reinforcing privacy and data protection through selective disclosure (European Commision, ٢٠٢٠).

٤. Digital Identity and Payment within the development of Open Banking concepts

Open Banking concept development is deeply connected with the evolution of digital identity and payment systems. Open Banking is the practice of exchanging financial data and services between financial institutions and third-party developers via Application Programming Interfaces (APIs) securely and transparently. This grants consumers and businesses greater control over their financial data and access to a broader array of services.

Digital identity and payment systems are fundamental to the development of Open Banking concepts. They improve security, facilitate innovative payment solutions, and enhance the user experience. However, addressing security, privacy, standardization, and regulatory issues is necessary for the successful integration of these components into the Open Banking framework.

٤,١ The evolution of open banking and Balancing Innovation and Security:

Following the ٢٠٠٨ financial crisis, the key regulatory concerns were compliance and financial stability. The second EU Payment Services Directive (PSD٢), on the other hand, moved its emphasis to supporting technological innovation and transforming the banking system. It established an open banking system, with the potential to expand into open finance. Banks must offer "access to account" and exchange customer and payment account information with authorized third parties under PSD٢. Once they have access to account information, new players will be able to enter not only the payments sector, but also other segments.PSD٢'s influence extends beyond legislative constraints, greatly speeding up the ongoing digitization of banking. This mandate upsets banks' formerly reliable revenue streams, prompting a shift in thinking from controlling to managing consumers' money. This shift emphasizes the shift away from traditional banking relationships and towards a more dynamic and diverse service landscape.

The shift to open banking is a global movement, although its consequences are influenced by regulatory settings, which include issues such as open finance and the data economy. Some countries, such as Australia and Singapore, are actively welcoming this change, while others are still evaluating the situation (Kooli, ٢٠٢٣).

Several driving forces are at work in the transformation: First: Technological Progress: Banks can use open banking to create a diverse set of Application Programming Interfaces (APIs) and services that go beyond statutory mandates. This paves the door for premium APIs, enabling data exchange practices in a variety of industries. Technology start-ups, as well as established incumbents and BigTechs, are entering the financial services industry to offer a wide range of products and services to consumers and companies directly. Second: Changes in Consumer Behavior: Open banking allows customers to gain access to a wider range of financial services, including accounts, mortgages, insurance, investments, and loans. This access allows for the provision of added value in the form of personalized services, creditworthiness assessments, and targeted financial advice. The success of open finance, however, is dependent on users being aware and prepared to provide third-party providers access to their financial data. Third: Shifting Customer Attitudes: Convenience, simplicity, cost savings, personalized services, and experience factors are increasingly important to consumers in their banking encounters. The COVID-١٩ pandemic has expedited the industry's move to digital banking channels, increasing competition and compressing profit margins (Kooli, ٢٠٢٣).

In essence, open banking and increasing client expectations are causing a dramatic transformation in the financial sector. PSD٢'s legislative shift, combined with technological improvements and changing consumer behavior, is encouraging innovation and competitiveness in the banking sector. This shift emphasizes the importance of banks adapting their strategy in order to remain competitive in a dynamic and continuously expanding financial ecosystem (Kooli, ٢٠٢٣).

٤,٢ The legal Impact of AI on Digital Payment Security:

Artificial intelligence refers to any device that can simulate cognitive functions similar to those of the human mind to successfully complete a task. In other terms, AI is a machine that can solve problems to attain a specific purpose. It is already having a significant impact in the finance and banking sectors, as well as the payments business. It is reasonable to say that it is piquing the interest of businesses all around the world. The payments landscape is rapidly expanding, fueled by changing technology and digital change across industries. Digital commerce has clearly extended beyond the desktop and even beyond mobile. The ability to pay anywhere, at any time will become increasingly common as the Internet of Things expands and customers become more connected at every level — from gadgets to apparel and appliances (Mrs. S. Deepalakshmi, ٢٠١٨).

Artificial intelligence will enhance and expedite this reality by leveraging machine learning to streamline payments at every level. The popularity of Alexa, Siri, Google Assistant, and Samsung's Bixby is altering how people engage with technology. Artificial intelligence is doing more than ever behind the scenes to process and protect payments. Criminals are increasingly using machine learning and bots to perpetrate online fraud, which presents a unique difficulty in companies that offer high-ticket items, such as the tourism industry (Mrs. S. Deepalakshmi, ٢٠١٨).

For decision making, most biometric identification solutions rely on AI-supported technology. Apple introduced powerful facial recognition technology in the new iPhone X in ٢٠١٧, and we anticipate that further applications of this "contactless identification" will emerge shortly. This will totally transform checkout operations and make online and in-store payments safer. We also anticipate that advanced identification technologies will reduce the need of physical cards and increase demand for virtualized payment instruments (Mrs. S. Deepalakshmi, ٢٠١٨).

٤,٣ The optimum Regulation of Cross-Border Payments and Remittances:

Taking Swiss Payment market as a matured digital payment environment, the introduction of mobile payment applications has significantly transformed the Swiss payment market over the past few years. This has resulted in an influx of new competitors and a rapid consolidation process. Existing electronic payment systems, some of which rely on credit or debit card schemes, facilitate point-of-sale payments in e-commerce and peer-to-peer (“P٢P”) transactions.

Certain payment applications are linked to traditional bank accounts with partner banks, enabling the payer-authorized execution of payments as bank transfers (Guberan, ٢٠٢٣).

New legislation governing cross-border payments and remittances will go into effect on January ١, ٢٠٢٠. Non-Swiss providers of cross-border financial services must abide by Swiss norms of conduct and, in some instances, register their client advisers in Switzerland. However, under Swiss law, Anti-Money Laundering obligations primarily pertain to financial intermediaries physically present in Switzerland and may not extend to foreign institutions operating internationally. However, the general criminal prohibition against money laundering remains in effect.

The authorization or licensing procedure for fund administrators differs between Swiss and foreign investment funds. The regulatory structure differentiates between open- and closed-ended collective investment schemes. The structures of open-ended schemes are contractual funds or investment companies with variable capital ("SICAV"). Structured as limited partnerships for collective investments ("LP") or investment companies with fixed capital ("SICAF"), closed-end schemes are not open to new investors. These distinctions are refined based on the type of investments, such as securities funds, real estate funds, traditional investment funds, and alternative investment funds, each of which adheres to distinct regulatory guidelines.

٥. FRA and CBE Egyptian Digital Identity Controls:

The Financial Regulatory Authority ("FRA") and the Central Bank of Egypt ("CBE") are two of Egypt's most significant regulatory bodies that oversee financial and banking operations. FRA and CBE play crucial roles in defining Egypt's financial digital identity landscape. Their regulations and supervision safeguard consumers and the integrity of the financial system by establishing a secure environment for digital financial services They have a significant impact on establishing and enforcing digital identity controls to ensure that digital financial transactions and services in the country are secure, authentic, and compliant. FRA regulates and oversees Egypt's non-bank financial markets. It emphasizes digital identity controls in Procedures for

Know Your Customer, Measures Against Money Laundering and the Financing of Terrorism, and standards for cyber security.

On the other Hand, CBE is responsible for maintaining price stability and overseeing financial institutions. It plays several roles in digital identity controls which include: Oversight of Payment Systems, and E-Payment Regulations. CBE may establish standards for digital banking services, including identity verification for online accounts and transactions.

In both the FRA and CBE contexts, digital identity controls encompass the Identity Verification, Biometric Authentication, Data Privacy, Electronic Signatures, implementing measures to prevent identity theft and fraud, such as monitoring transaction patterns in real-time, and International Compliance.

٥,١ Enactment of FRA digital identity regulations:

More than a year after the enactment of the Law Regulating and Developing the Use of Financial Technology in Non-Banking Financial Activities (the "FinTech Law") In Egypt. The Financial Regulatory Authority ("FRA") recently issued three executive decisions to operationalize the law. The first decision outlines the requirements for equipment, technological infrastructure, information systems, and necessary protection measures for the use of financial technology. The second decision establishes the criteria for creating digital identities, digital contracts, and digital ledgers. The last decision permits the creation of a register for service outsourcing providers.

In this evolving landscape, digital identity and authentication have emerged as crucial components in the realm of financial services. Digital identity refers to the digital representation of an individual's identity, enabling verification and authentication for accessing online services and conducting financial transactions (World Economic Forum, ٢٠١٦).The acceptance of digital identity as a trusted means of identification has opened new avenues for financial institutions to provide personalized and secure services to their customers (EUR-Lex, ٢٠٢٠).

One of the key provisions introduced by the New Decisions pertains to the regulations of digital identity. It is defined as, "Any technically processed data related to an identifiable individual or entity, either directly or indirectly, by associating this data with other information such as name, voice, image, identification number, or identity indicators over the global communication network (internet). This data should facilitate the evaluation and authentication of transactions made through digital platforms associated with non-banking financial activities.

The New decree issued by FRA in Egypt mandated the use of at least four elements from the "possession factor group." These must include personal identification, email address, mobile phone number, and device number. Additionally, there should be at least three elements from the "presence and vitality factor group," amongst which are facial biometric features, response vitality, and geographic location indicators, amongst other requirements. The New Decisions classified digital identity into three trust levels, allowing service providers to gauge the type of operation based on its risk. Each level encompasses a minimum of the aforementioned elements. The trust levels are: First: Basic Trust Level: Required for low-risk operations. Second: General Trust Level: Involves the minimum factors required at the Basic Trust Level, along with the possession of a non-cash payment account. This level is required for medium-risk operations. Third: High Trust Level: Encompasses the minimum factors of the General Trust Level, with the addition of an accredited electronic signature. This level is essential for high-risk operations. (THEBES, ٢٠٢٣).

٥,٢ The rise of regulatory sandbox:

The concept of a regulatory sandbox has been introduced in several jurisdictions, including the UK, Australia, the US, Hong Kong, Singapore, the Netherlands, Canada, and Egypt as a potential solution for regulating FinTech businesses. Regulatory sandboxes offer a temporary relaxation or exemption from regulatory requirements, allowing FinTechs to test new products and business models under regulatory supervision. This approach aims to strike a balance between promoting financial innovation and ensuring regulatory compliance. The collaborative environment within a sandbox allows ongoing dialogue between regulators and FinTech firms, fostering mutual knowledge exchange (Rugilo, ٢٠١٩).

Regulatory sandboxes are part of the solution to address the trade-off between sound financial regulations and fostering innovation. They provide a controlled space for FinTechs to innovate and test their products while maintaining regulatory oversight. Additionally, innovation hubs, which offer preliminary regulatory guidance, complement the sandbox concept (Rugilo, ٢٠١٩).

The theoretical basis of sandbox concepts originates from the IT sector, where isolated testing environments are used to identify and prevent system malfunctions. The concept was adopted in the financial regulatory context by the UK's Financial Conduct Authority in ٢٠١٥ and has since spread across countries. While sandboxes vary in design, they share key characteristics and components, such as offering a safe space for testing, fostering innovation, and facilitating information exchange between regulators and firms (Rugilo, ٢٠١٩).

For example, in Germany, although no comparable initiative exists, there is a growing interest in FinTech regulation. Workshops, task forces, and initiatives demonstrate the country's interest in strengthening the dialogue between policymakers, regulators, and the FinTech industry. The German government is also developing strategies to establish the country as a FinTech hub within the European Union and is considering flexible regulatory frameworks for crypto-assets (Rugilo, ٢٠١٩).

Overall, regulatory sandboxes have the potential to lower regulatory barriers, accelerate market introductions of innovative services, and provide regulators with valuable insights for adapting regulations to the FinTech landscape. While Germany is yet to implement a sandbox, ongoing efforts and initiatives signal the increasing importance of FinTech markets and the need for suitable regulatory approaches.

The framework of necessary conditions for a regulatory sandbox involves a comprehensive set of factors spanning legal, regulatory, stakeholder, capacity, market, regulatory regime, industry maturity, country-level, and firm-level considerations. This framework aids in evaluating whether a regulatory sandbox is suitable for FinTech and RegTech regulation and whether the necessary conditions are met.

Jeník and Lauer (٢٠١٧) introduced a framework of necessary conditions for effectively implementing a regulatory sandbox in FinTech and RegTech regulation. The identified conditions encompass various aspects (Lauer, ٢٠١٧): First: Legal and Regulatory Framework: This includes the regulator's mandate to operate a sandbox and their regulatory philosophy towards FinTech. The distinction between rules-based and principles-based regulation is crucial. Principles-based philosophy supports innovation and competition and is well-suited for a sandbox, whereas rules-based regulation involves strict adherence to predefined rules. Second:

Stakeholder Ecosystem: The collaboration among different regulatory authorities involved in FinTech regulation is important for congruency and to avoid fragmented and conflicting regulation. Inclusion of all relevant regulators, such as financial, technological, and telecommunication regulatory bodies, enhances regulatory effectiveness. Third: Capacity and Resources: Running a sandbox requires dedicated human resources with both regulatory and FinTech acumen. Adequate financial resources are needed for the functioning of a sandbox. The resource-intensive nature of sandboxes underscores the importance of proper resource allocation. Fourth: Market Conditions: Market conditions encompass both supply and demand factors. On the supply side, the number, type, and growth rate of FinTech firms and products are considered. On the demand side, the size of the potential market and the proportion of financially excluded individuals play a role. Building on this foundation, the World Bank (٢٠٢٠) expanded the framework with two notable additions. Fifth: Regulatory Regime Factors: This includes the maturity of the financial services' regulatory regime, affiliation with international associations for knowledge exchange, regulator maturity to respond to changes, transparency, and trust in the regulator's actions and outcomes. Sixth: FinTech Industry Maturity: The level of maturity and growth of the FinTech industry, as well as the types of firms involved, were identified as key factors. A growing and developing FinTech industry with a clear trajectory is essential for a successful regulatory sandbox.

In addition, there are some additional categories emerged from a review of existing literature such as Country-Level Conditions: since Government policies, financial inclusion, technological innovation, SME development, financial system development,. cognitive-powered RegTech plays in helping banks manage their growing regulatory burdens as it describes how regulatory technology (RegTech) has been integrated with cognitive computing and artificial intelligence (AI) technologies. By merging cutting-edge AI tools like machine learning, natural language processing, and data analytics, cognitive regtech goes one step further in raising the level of sophistication, accuracy, and efficiency of regulatory compliance and risk management duties. It makes it possible to navigate challenging and changing regulatory environments using automated and intelligent decision-making. With rising expenses and non-compliance concerns, financial institutions are faced with increased regulatory challenges where RegTech businesses help with compliance, but the special complexity of finance necessitates a distinct approach. Intricate regulatory complications are being handled by the adoption of cognitive technology (Peter Collins, ٢٠١٧).

٥,٣ The implementation of CBE for FinTech and Reg Tech startups:

The CBE Regulatory Sandbox, established in May ٢٠١٩, offers a controlled testing space for startups to trial creative business models and delivery methods with relaxed regulations, thus mitigating risks linked to disruptive technologies. Its key aims are to promote fintech and innovation, navigate regulatory ambiguity, expedite market entry, and cultivate investor confidence. The sandbox journey involves five main stages. The CBE Regulatory Sandbox procedure includes the following stages: Application as Applicants submit an online form on the CBE's official website. Prior to approval, the regulator evaluates applications based on predetermined criteria. Preparation phase: The applicant and regulator determine prototype testing parameters in collaboration. Experimentation Phase: The applicant attempts their project while the regulator observes their development. Graduation Phase: Upon completion of testing or the agreed-upon period, the applicant submits a report delineating test results to the regulator (FinTech Egypt - CBE, ٢٠٢١).

To qualify for the Regulatory Sandbox, applicants must satisfy the following requirements: Focus on financial technology (FinTech): The project lies within the scope of financial technology (FinTech). Real Innovation: The project presents concepts or methods that are truly innovative. Customer Benefits: The initiative provides customers with tangible benefits. Sandbox Necessity where Sandbox testing is essential for the endeavor. Readiness for Sandbox Testing: The applicant is willing and able to participate in sandbox testing. Digital Transformation and Financial Inclusion: The project supports digital transformation and financial inclusion initiatives (FinTech Egypt - CBE, ٢٠٢١).

The regulatory laboratory for the CBE functions in cohorts: Cohort ١ (July ٢٠١٩): Introduced as a thematic pilot, it centered on E-KYC for mobile wallets and streamlined digital consumer onboarding. Cohort ٢ (November ٢٠٢٠): An open-theme cohort comprising numerous FinTech initiatives and trends (FinTech Egypt - CBE, ٢٠٢١).

٦. Findings, Conclusions, and Recommendations

٦,١ Findings:

A significant problem in the digital ecosystem is ensuring the precision and dependability of identity verification and authentication procedures. Due to the increased sharing of personal information online, there are considerable hazards of identity theft and impersonation. The necessity for reliable identity verification systems is highlighted by liability, accountability, and data protection concerns related to these processes. Utilizing techniques like address verification and biometric data may build client confidence, stop fraud, and guarantee secure transactions.

Unique legal difficulties arise when enrolling kids in online services, notably when securing the required guardians' consent. To avoid privacy violations and potential harm to minors, compliance with age-specific laws and international norms is essential. Children's privacy, safety, and security when using digital products and services are protected by initiatives like the EU's Digital Services Act (“DSA”) and code of conduct on age-appropriate design. Collaboration between business, government, civil society, and children is essential to the success of this initiative.

Legal capability, or the power to make contracts with legal force, is essential for digital identity in the online world. Users' interactions and behaviors are influenced by the difference in the construction of identities online and offline. Because of the freedom of expression and emerging technologies, cyberspace offers a platform for people to create unique versions of themselves. To account for these distinctive traits, legal issues relating to digital identification must change.

In order to process personal data, the General Data Protection Regulation (“GDPR”) emphasizes clear user agreement. Platforms for managing consent (“CMPs”) automate the process of obtaining consent and guarantee compliance. While laws like the California Consumer Privacy Act (“CCPA”) and the General Data Protection Regulation (“GDPR”) specify consent criteria for various reasons, best practises call for the adoption of CMPs, the use of user-friendly banner designs, and simplifying consent across numerous websites.

The NIST SP ٨٠٠-٦٣-٣ rules offer a complete framework for managing risk, digital identity, and authentication. The efficiency of identity verification and authentication is measured at several assurance levels (IAL and AAL). These recommendations place a strong emphasis on risk assessment, component-by-component evaluation, and technology-driven risk determinations. When making technology-related decisions, organizations are recommended to put security and risk management first.

A consistent framework for electronic identity, authentication, and trust services in the EU is established under the eIDAS Regulation. By allowing use of national electronic identification schemes (eIDs) for online services, it facilitates cross-border transactions. The law strengthens the legitimacy of digital services and encourages citizens and businesses to adopt them. The compliance of the law with technology improvements is ensured through stakeholder engagements and assessments.

The study entails also the effects of digital identity regulations put in place by the Financial Regulatory Authority (FRA) and the Central Bank of Egypt (CBE) on the Egyptian banking industry.

The laws of the FRA and CBE are essential for creating a safe digital financial ecosystem.

The study shows how digital identity controls, such as biometric authentication and data protection safeguards, are put into practice to guarantee safe and legal digital financial transactions

The emergence of regulatory sandboxes, like the CBE Regulatory Sandbox, gives FinTech and RegTech businesses a regulated testing environment to develop while preserving regulatory monitoring.

٦,٢ Conclusions:

The need for seamless and secure online interactions, as well as the development of new technologies, have created a difficult environment for digital identification and authentication. Therefore, the research results support the following major conclusions:

١. Choosing Between Security and Convenience: A significant difficulty is ensuring the precision and dependability of digital identity verification and authentication systems. Businesses balance user comfort and security as they employ reliable verification methods.

Increased trust is provided by procedures like address verification and biometric authentication while fraud and identity theft are protected.

٢. Online Child onboarding Protection: The legal environment regarding child onboarding necessitates close consideration. With programmers like the EU's Digital Services Act (“DSA”) and age-appropriate design code attempting to protect minors' privacy, safety, and security in digital settings, compliance with age-specific laws and international standards is crucial. Success depends on coordinated efforts from business, government, civil society, and kids.

٣. Legal Capacity and Digital Identity: The online environment has a distinctive influence on identity development, setting digital identity apart from real-world identity. To ensure secure, equitable, and legally binding digital interactions, the impact of legal capability on digital identification is crucial. Effectively handling legal issues requires an understanding of the unique features of the online environment.

٤. Regulations like the GDPR and CCPA highlight how crucial user consent is for processing personal data. Organizations should put a priority on user-friendly design and cross-website consent alignment while effective consent management platforms (“CMPs”) streamline compliance, user experience, and transparency.

٥. An extensive framework for managing digital identities and authentication procedures is provided by NIST's Digital Identity Guidelines. To reduce possible hazards, organizations must give priority to risk assessments, component evaluations, and technology-driven decisions. The sector may successfully traverse evolving authentication challenges by focusing on security and following rules.

٦. A uniform framework for electronic identity, authentication, and trust services in the EU is introduced by the eIDAS Regulation. In order to promote the adoption of secure digital contacts, it attempts to establish confidence and legal validity for electronic interactions among member nations. The regulation is continually assessed to guarantee its applicability in light of new technology developments.

٧. The dynamic interaction between technological advancements and legal issues in the area of digital identity and authentication is changing how people and entities communicate online. Collaboration between policymakers, business leaders, and technology experts is essential for assuring secure, seamless, and reliable digital transactions for all stakeholders as technological developments continue to transform the digital landscape.

٦,٣ Recommendations:

Below are some recommendations that can help Egypt create a safe, dependable, and user-friendly digital identity ecosystem that promotes innovation, economic growth, and digital inclusion while placing a high value on user privacy and data security.

١. Work with financial regulatory organizations like the FRA and CBE to improve the rules already in place for digital identity and authentication in order to promote a safe and uniform digital ecosystem, rules should be updated and aligned with global best practices.

٢. Encourage collaborations between government organizations, financial institutions, technology suppliers, and industry groups to jointly address problems with digital identification and authentication with cooperation promotion in the creation and deployment of ground-breaking solutions that place a focus on security, user experience, and legal compliance.

٣. Create a thorough national digital identity plan that outlines a timeline for putting into place safe, reliable, and user-focused digital identification solutions.

٤. Launch public awareness campaigns to inform people about the value of digital identity security, data protection, and safe online practices to Advocate for appropriate use of digital services and the value of informed permission when processing personal data.

٥. Define clear standards for Egypt-based websites and digital platforms to follow when implementing compliant and user-friendly consent management platforms (CMPs). Encouraging companies to adopt consent procedures that are compliant with international laws like the GDPR, which ensures openness and user control over their personal data.

٦. Adopt the NIST Digital Identity Guidelines or equivalent standards to determine the degree of risk related to digital identity, authentication, and trust services. This is to develop user-friendly security and convenience methods by putting in place the right amount of identity assurance and authentication.

٧. Invest in projects geared towards increasing cybersecurity, authentication, and digital identity technologies by offering incentives to startups and IT companies developing digital identification solutions, you may support an ecosystem of innovation.

٨. Set up procedures for routinely assessing and changing digital identity laws and technologies in response to changing cyberthreats and technological developments. This requires to keep an eye on worldwide developments in the fields of digital identification and authentication to make sure Egypt stays at the forefront of user-friendly security measures.

٩. Invest in training programs and initiatives to build the capacity of government officials, regulators, financial institutions, and technology professionals to improve their comprehension of digital identity technologies, legal ramifications, and best practices.

Bibliography

Biometricupdate. (٢٠٢٢, May ١٢). *Age verification and digital wallets for minors: EU launches strategy for online child safety*. Retrieved from biometricupdate: https://www.biometricupdate.com/٢٠٢٢٠٥/age-verification-and-digital-wallets-for-minors-eu-launches-strategy-for-online-child-safety

Chamberlains. (٢٠٢٣). *Contract Law – Capacity*. Retrieved from chamberlains.com.au: https://chamberlains.com.au/contract-law-capacity/

Craggs, J. (٢٠٢٣, June ٥). Keeping on Track: Fairness and Bias in AI Banking Systems.

Cryptomathic. (٢٠٢٢, April ٠٤). *Digital Identity and eIDAS in Banking*. Retrieved from Cryptomathic: https://www.cryptomathic.com/news-events/blog/digital-identity-and-eidas-in-banking

Cucko, S. (٢٠٢١, September ٢٠٢١). Towards the classification of Self-Sovereign Identity properties. ٢-٣.

Deloitte. (٢٠٢٢, Feb ١٦). *Earning digital trust: Where to invest today and tomorrow*. Retrieved from Deloitte: https://www٢.deloitte.com/xe/en/insights/topics/digital-transformation/digital-trust-solutions.html

Eduard Rupp, E. S. (٢٠٢٢). *Leave No Data Behind – Empirical Insights into Data Erasure from Online Services.*

eMudhra Editorial. (٢٠٢١, December ١٤). *Digitally Onboard Your Banking Customers*. Retrieved from eMudhra: https://emudhra.com/blog/digitally-onboard-your-banking-customers

EUR-Lex. (٢٠٢٠). *Digiatl Identity* . Retrieved from EUr-Lex Access to uropean union Law: https://eur-lex.europa.eu/EN/legal-content/glossary/digital-identity.html

European Commision . (٢٠٢٠, OCT). *eIDAS Regulation* . Retrieved from Official Web Site of European Union: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

Ewa Michalkiewicz-Kadziela, F. o. (٢٠٢٢, Jan ١٤). Legal boundaries of digital identity creation. *Internet Policy Review*.

Faceonlive. (٢٠٢٣, June ٢١). *Identity Verification: Boost Security & Trust – The Ultimate Guide*. Retrieved from faceonlive: https://faceonlive.com/identity-verification-boost-security-trust-the-ultimate-guide/

FinTech Egypt - CBE. (٢٠٢١). *EgypT FinTech Landsacpe Report.* CBE.

Frei, C. (٢٠٢٣, February ٢٥). Open Banking: Opportunities and Risks. *Springer*, ١٧٨-١٨٠.

Frontiers. (٢٠٢٢, March ١٤). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? *Frontiers*.

Guberan, L. M. (٢٠٢٣). *Definitive global law guides offering - comparative analysis from top-ranked lawyers.* Switzerland: Law & Practice.

Hoekman, B. (٢٠٢١, September). Digitalization, International Trade, .

Jason E. (٢٠٢٠, September ٢٤). *8 Benefits of EKYC in Digital Onboarding Process For Banks.* Retrieved from https://www.linkedin.com/pulse/٨-benefits-ekyc-digital-onboarding-process-banks-jason-edwards/

Jens Strüker, N. U. (٢٠٢١, Septemberf). Self-Sovereign Identity - Foundations, Applications, and Potentials of Portable Digital Identities. ١٣-١٥.

Kooli, T. W. (٢٠٢٣). *The finnTech disruption Hoe financial Innovation Is Transforming the banking Industry.*

Laatikainen, G. K. (٢٠٢١). Self-Sovereign Identity Ecosystems : Benefits and Challenges. *Informaatioteknologian tiedekunta*.

Lauer, I. J. (٢٠١٧, October). Regulatory Sandboxes and Financial Inclusion. *CGAP*.

Martin Hasal, J. N. (٢٠٢١, June ٣). Chatbots: Security, privacy, data protection, and social aspects. *Wiley*.

Mrs. S. Deepalakshmi, B. M. (٢٠١٨, Oct). Impact of Artificial Intelligence in E-Payments. *Rajapalayam Rajus' College*.

Myers, K. (٢٠٢٣). Digital Insanity: Exploring the Flexibility of NIST Digital Identity Assurance Levels. (pp. ٢-٦). Maryland,USA: ICCWS.

National institute of Standars and Technology NIST. (٢٠١٧). *Digital Identity Guidliness.* NIST special Publications.

Nicol, J. (٢٠٢١, May ٢٠). *How Digital Identity Processing Can Create A Faster, More Secure Customer Onboarding Process.* Retrieved from https://www.forbes.com/sites/forbestechcouncil/٢٠٢١/٠٥/٢٠/how-digital-identity-processing-can-create-a-faster-more-secure-customer-onboarding-process/

NIST ٨٠٠-٦٣-٣. (٢٠١٧). *Digital identity guidliness.*

OECD. (٢٠٢١). Artificial Intelligence, Machine Learning and Big Data in Finance. *OECD*.

Peter Collins, I. W. (٢٠١٧, June ٩). *Can cognitive RegTech help banks meet growing regulatory burdens?* Retrieved from Medium : https://medium.com/@InnFin/can-cognitive-regtech-help-banks-meet-growing-regulatory-burdens-٤٠bf٥٨a٧ac٣٨

Rugilo, J. M. (٢٠١٩, March). The Predicament of FinTechs in the Environment of Traditional Banking Sector Regulation – An Analysis of Regulatory Sandboxes as a Possible Solution. *Credit and Capital Markets*.

Secure Privacy . (٢٠٢٣, January ٢٦). *Data Privacy and Protection: A Guide to Consent Management Best Practices*. Retrieved from Secure Privacy : https://secureprivacy.ai/blog/guide-to-consent-management-best-practices

Springer. (٢٠٢٢, November). Artificial Intelligence-Based OCR. *Springer*.

THEBES, C. (٢٠٢٣, August). EGYPT Legal Updates. *AUGUST 2023 Week 2*, p. ٤.

Utz, C. (٢٠١٩). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *ACM*.

World Economic Forum. (٢٠١٦). *A Blueprint for Digital Identity:The Role of Financial Institutions in Building Digital Identity*. An Industry Project of the Financial Services Community | Prepared in collaboration with Deloitte.