



LEGAL DIGITAL FINANCE CERTIFICATE

FOUNDATIONAL LEVEL - MODULE 2 – PHASES OF FINANCIAL TRANSACTIONS
[IDENTIFY - VERIFICATION – AUTHENTICATION]

By : Dr. Sherif Mohsen Shaltout (PhD)

MODULE 2- PHASES OF FINANCIAL TRANSACTION [IDENTITY – VERIFICATION – AUTHENTICATION]

01

**LEGAL CAPACITY AND
DIGITAL IDENTITY**

02

**VERIFICATION &
AUTHENTICATION PHASE**

03

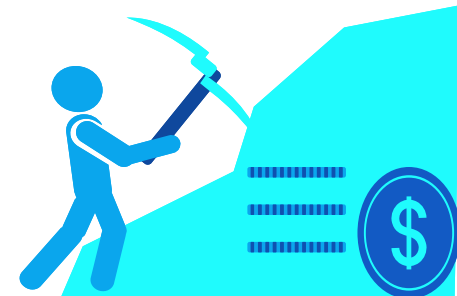
**INTRODUCTION TO RISK
MANAGEMENT - PRIVACY**

04

INTRODUCTION TO AI

05

**INTRODUCTION TO
RESPONSIBLE AI**



HOMONYMS IN FINANCE AND LAW: UNDERSTANDING CONTEXTUAL MEANING



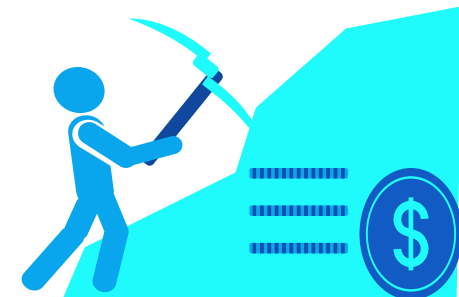
THE TERM **(LIABILITIES)** HAS DIFFERENT MEANINGS IN FINANCE AND LAW.

IN FINANCE:

- **LIABILITIES** REPRESENT THE FINANCIAL OBLIGATIONS A COMPANY OWES TO ITS CREDITORS.
- THESE OBLIGATIONS ARISE FROM PAST TRANSACTIONS, SUCH AS PURCHASES OF GOODS OR SERVICES, LOANS, TAXES, AND EMPLOYEE SALARIES.
- LIABILITIES ARE CONSIDERED "DEBTS" AND ARE LISTED ON A COMPANY'S BALANCE SHEET UNDER THE "LIABILITIES" SECTION.

IN LAW:

- **LIABILITIES** REFERS TO THE PARTIES INVOLVED IN A LEGAL DISPUTE.
- THESE PARTIES ARE ALSO KNOWN AS "LITIGANTS" OR "DISPUTANTS."
- THEY ARE THE INDIVIDUALS OR ENTITIES WHO ARE BRINGING OR DEFENDING A LAWSUIT AGAINST EACH OTHER.



HOMONYMS IN FINANCE AND LAW: UNDERSTANDING CONTEXTUAL MEANING



THE TERM **INTERMEDIARY** HAS DIFFERENT MEANINGS IN FINANCE AND LAW.

IN FINANCE:

INTERMEDIARY REFERS TO A PERSON OR ENTITY THAT ACTS AS A MIDDLEMAN IN A FINANCIAL TRANSACTION.

THEY FACILITATE THE EXCHANGE OF GOODS, SERVICES, OR MONEY BETWEEN TWO OR MORE PARTIES.

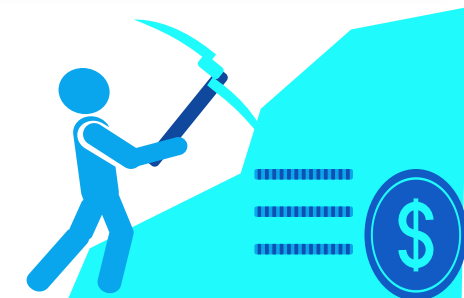
EXAMPLES OF INTERMEDIARIES IN FINANCE INCLUDE BROKERS, DEALERS, AND UNDERWRITERS.

IN LAW:

(INTERMEDIARY) REFERS TO A PERSON OR ENTITY THAT HELPS TO RESOLVE A DISPUTE BETWEEN TWO OR MORE PARTIES.

THEY ACT AS A NEUTRAL THIRD PARTY AND WORK TO FIND A COMPROMISE THAT IS ACCEPTABLE TO BOTH SIDES.

EXAMPLES OF INTERMEDIARIES IN LAW INCLUDE MEDIATORS, ARBITRATORS, AND CONCILIATORS.



PHASES OF FINANCIAL TRANSACTION

01

IDENTIFICATION

02

VERIFICATION

03

AUTHENTICATION

04

AUTHORIZATION

05

ENTRY

06

VALIDATION

07

DISPUTE RESOLUTION



LECTURE - 1

IDENTITY , VERIFICATION , AUTHENTICATION THE INTERPLAY OF FINANCE, LAW, AND TECHNOLOGY

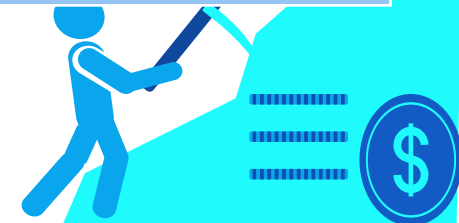
LEGAL CAPACITY Vs. PERSONAL LEGAL HOOD

IDENTITY RECOGNITION METHODS (TRADITIONALLY Vs. DIGITAL)

EKYC AS A DIGITAL IDENTITY CONCEPT

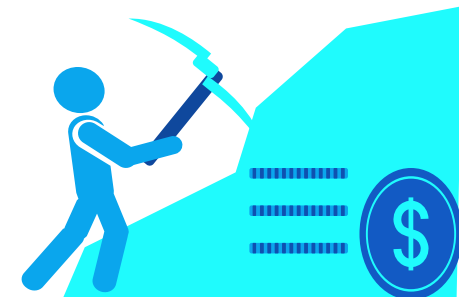
SOCIAL SELF THEORY

LEGAL CAPACITY CHALLENGES IN DIGITAL IDENTITY



1- IDENTIFICATION

- **FINANCE:**
 - IDENTIFYING PARTIES INVOLVED IN A TRANSACTION (E.G., SENDER, RECIPIENT, FINANCIAL INSTITUTIONS).
 - MAINTAINING ACCURATE CUSTOMER RECORDS FOR FINANCIAL ACCOUNTING AND REPORTING.
- **DIGITAL:**
 - UTILIZING BIOMETRICS (FINGERPRINT, FACIAL RECOGNITION), DIGITAL SIGNATURES, AND UNIQUE IDENTIFIERS FOR SECURE IDENTIFICATION.
 - IMPLEMENTING DIGITAL ONBOARDING PROCESSES FOR NEW CUSTOMERS.
- **LAW:**
 - DATA PRIVACY REGULATIONS GOVERNING THE COLLECTION, STORAGE, AND USE OF PERSONAL INFORMATION.
 - LEGAL REQUIREMENTS FOR CUSTOMER IDENTIFICATION PROCEDURES.



THE IMPORTANCE OF ACCURATE FINANCIAL RECORDS AND TRANSACTION TRACKING

UNDERSTANDING TRANSACTIONS:

TRACKING MONEY FLOW:

IDENTIFYING PARTIES INVOLVED (SENDER, RECIPIENT, FINANCIAL INSTITUTIONS) ALLOWS FOR:

- FRAUD PREVENTION: SUSPICIOUS ACTIVITY CAN BE FLAGGED AND STOPPED.
- RECONCILIATION: ENSURES ACCURATE ACCOUNTING AND AVOIDS DISCREPANCIES.
- TAX COMPLIANCE: PROPER REPORTING AND COMPLIANCE ARE FACILITATED.

MAINTAINING ACCURATE CUSTOMER RECORDS:

FINANCIAL STATEMENTS: ACCURATE RECORDS ARE CRUCIAL FOR GENERATING RELIABLE FINANCIAL STATEMENTS.

RISK MANAGEMENT: CUSTOMER FINANCIAL HISTORY HELPS ASSESS CREDITWORTHINESS AND MANAGE RISKS.

REGULATORY COMPLIANCE: ACCURATE RECORDS ENSURE ADHERENCE TO REGULATIONS FOR AUDITING AND REPORTING.



HOW TECHNOLOGY TRANSFORMS IDENTIFICATION AND CUSTOMER ACQUISITION



BIOMETRICS AND DIGITAL SIGNATURES:

- CAPTURING, STORING, AND VERIFYING USER DATA.
- FINGERPRINT SCANNERS, FACIAL RECOGNITION SOFTWARE, AND DIGITAL SIGNATURE ALGORITHMS ALL OPERATE WITHIN THE DIGITAL REALM.

DIGITAL ONBOARDING:

- USING ONLINE PLATFORMS AND DIGITAL TOOLS TO GATHER CUSTOMER INFORMATION, VERIFY IDENTITY, AND COMPLETE ACCOUNT SETUP.
- PAPER FORMS, PHYSICAL DOCUMENTS, AND IN-PERSON INTERACTIONS ARE REPLACED WITH DIGITAL COUNTERPARTS.

ACCESSIBILITY AND CONVENIENCE:

- DIGITAL TOOLS ARE READILY ACCESSIBLE TO USERS FROM ANYWHERE WITH AN INTERNET CONNECTION.

DATA MANAGEMENT:

- THE INFORMATION COLLECTED THROUGH THESE METHODS IS STORED AND MANAGED DIGITALLY, ENABLING EFFICIENT DATA ANALYSIS, RECORD-KEEPING, AND COMPLIANCE WITH REGULATIONS.

SEAMLESS INTEGRATION:

- ARE OFTEN INTEGRATED WITH ONLINE PLATFORMS AND APPLICATIONS, ALLOWING FOR SECURE LOGINS, DOCUMENT SIGNING, AND OTHER DIGITAL TRANSACTIONS.

AUTOMATION AND EFFICIENCY:

- DIGITAL ONBOARDING PROCESSES LEVERAGE DIGITAL TOOLS AND AUTOMATION TO STREAMLINE CUSTOMER ACQUISITION AND ACCOUNT SETUP, REDUCING MANUAL TASKS AND PAPER-BASED PROCESSES.



WHY SECURE IDENTIFICATION MATTERS IN LAW

AML/KYC REGULATIONS

ANTI-MONEY LAUNDERING (AML) AND KNOW YOUR CUSTOMER (KYC) REGULATIONS ARE LEGAL MANDATES

THEY ARE ESTABLISHED BY LEGISLATIVE BODIES OR REGULATORY AUTHORITIES.

THESE REGULATIONS REQUIRE FINANCIAL INSTITUTIONS AND OTHER DESIGNATED BUSINESSES TO IMPLEMENT ROBUST CUSTOMER VERIFICATION PROCEDURES.

LEGAL BASIS:

COMBAT MONEY LAUNDERING, TERRORIST FINANCING, AND OTHER ILLEGAL ACTIVITIES THAT THREATEN FINANCIAL STABILITY AND SECURITY.

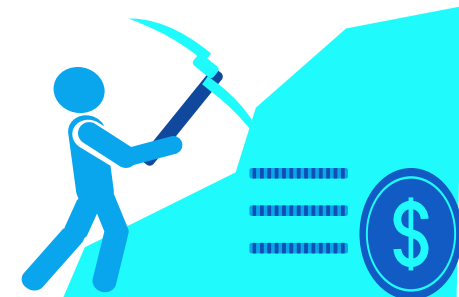
SAFEGUARD INDIVIDUALS FROM FRAUD AND SCAMS BY ENSURING THEY ARE WHO THEY CLAIM TO BE.

FOSTER TRANSPARENCY AND ENABLE THE IDENTIFICATION OF SUSPICIOUS ACTIVITY.

CONSEQUENCES OF NON-COMPLIANCE:

Failure to adhere to these regulations can result in significant legal repercussions

- **Financial Losses:**
- **Regulatory Penalties:**



VERIFICATION



• FINANCE:

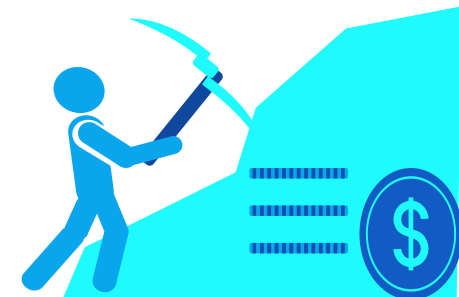
- CONFIRMING THE AUTHENTICITY AND VALIDITY OF IDENTIFIED PARTIES AND INFORMATION PROVIDED.
- PREVENTING FRAUDULENT TRANSACTIONS AND UNAUTHORIZED ACCESS TO FINANCIAL ACCOUNTS.

• DIGITAL:

- EMPLOYING DOCUMENT SCANNING TOOLS, DATA VALIDATION ALGORITHMS, AND THIRD-PARTY VERIFICATION SERVICES.
- UTILIZING DIGITAL CERTIFICATES AND SECURE COMMUNICATION CHANNELS TO ENSURE DATA INTEGRITY.

• LAW:

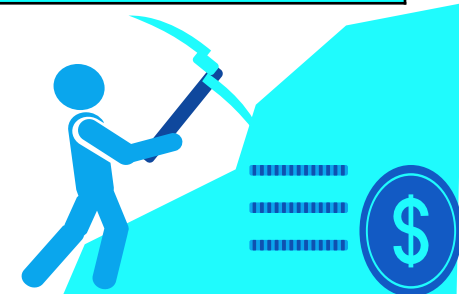
- ANTI-MONEY LAUNDERING (AML) AND KNOW YOUR CUSTOMER (KYC) REGULATIONS MANDATING CUSTOMER VERIFICATION PROCEDURES.
- LEGAL BASIS FOR VERIFICATION REQUIREMENTS, INCLUDING AGE RESTRICTIONS AND COMPLIANCE WITH SANCTIONS LISTS.
- LEGAL CONSEQUENCES OF INADEQUATE VERIFICATION, POTENTIALLY LEADING TO FINANCIAL LOSSES AND REGULATORY PENALTIES.



VERIFICATION FINANCE

Goal: Ensure financial transfers are accurate and intended

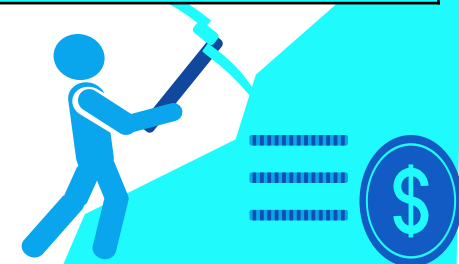
SECURITY MEASURE	DESCRIPTION	EXAMPLE
IDENTITY VERIFICATION	CONFIRMING THE PARTIES INVOLVED ARE WHO THEY CLAIM TO BE.	VERIFYING ACCOUNT HOLDER NAMES, SOCIAL SECURITY NUMBERS, OR OTHER IDENTIFYING INFORMATION.
DATA ACCURACY VERIFICATION	ENSURING ALL TRANSACTION DETAILS (AMOUNT, ACCOUNT NUMBERS) ARE CORRECT.	CHECKING FOR INCONSISTENCIES IN ENTERED DATA.



VERIFICATION FINANCE

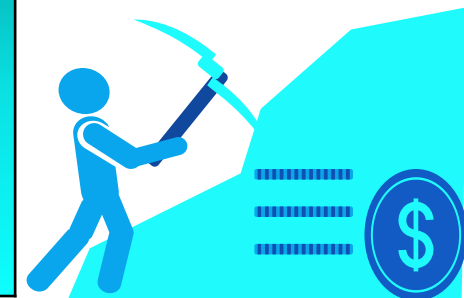


SECURITY MEASURE	DESCRIPTION	EXAMPLE
SECOND-FACTOR AUTHENTICATION (2FA)	REQUIRING AN ADDITIONAL VERIFICATION STEP BEYOND PASSWORD.	VERIFYING LOGIN ATTEMPTS THROUGH A CODE SENT TO YOUR PHONE OR FINGERPRINT SCAN.
DEVICE RECOGNITION	IDENTIFYING AUTHORIZED DEVICES USED TO ACCESS ACCOUNTS.	ALERTING YOU IF SOMEONE TRIES TO LOG IN FROM AN UNRECOGNIZED DEVICE.
SECURE COMMUNICATION CHANNELS	ENCRYPTING DATA TRANSMISSION TO PREVENT INTERCEPTION.	USING SECURE PROTOCOLS (HTTPS) FOR ONLINE BANKING TRANSACTIONS



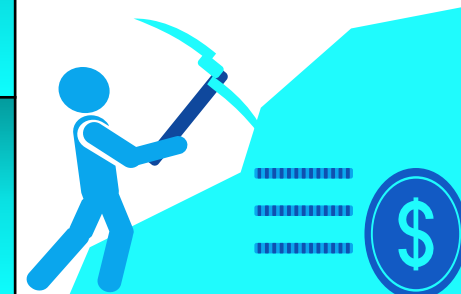
VERIFICATION DIGITAL

TASK	DIGITAL PERSPECTIVE
EMPLOYING DOCUMENT SCANNING TOOLS	<ul style="list-style-type: none">- USE DOCUMENT SCANNING TOOLS TO SCAN PHYSICAL DOCUMENTS INTO DIGITAL FORMATS.- THE SCANNED DOCUMENT CAN THEN BE PROCESSED AND STORED ELECTRONICALLY.
DATA VALIDATION ALGORITHMS	<ul style="list-style-type: none">- IMPLEMENT DATA VALIDATION ALGORITHMS TO CHECK THE ACCURACY AND COMPLETENESS OF THE DATA.- THIS CAN HELP TO IDENTIFY ERRORS AND INCONSISTENCIES IN THE DATA.
THIRD-PARTY VERIFICATION SERVICES	<ul style="list-style-type: none">- USE THIRD-PARTY VERIFICATION SERVICES TO VERIFY THE AUTHENTICITY OF DATA.- THESE SERVICES CAN HELP TO ENSURE THAT THE DATA IS COMING FROM A TRUSTED SOURCE.
UTILIZING DIGITAL CERTIFICATES AND SECURE COMMUNICATION CHANNELS	<ul style="list-style-type: none">- USE DIGITAL CERTIFICATES TO ENCRYPT DATA AND AUTHENTICATE THE SENDER AND RECEIVER.- THIS CAN HELP TO PROTECT THE DATA FROM UNAUTHORIZED ACCESS AND MODIFICATION.- USE SECURE COMMUNICATION CHANNELS TO TRANSMIT DATA.- THESE CHANNELS USE ENCRYPTION AND OTHER SECURITY MEASURES TO PROTECT THE DATA FROM INTERCEPTION.



VERIFICATION LAW

ASPECT	DESCRIPTION
REGULATIONS	ANTI-MONEY LAUNDERING (AML) AND KNOW YOUR CUSTOMER (KYC)
LEGAL BASIS	ESTABLISHED BY GOVERNMENTS AND FINANCIAL REGULATORY BODIES
PURPOSE	ENSURE FINANCIAL SECURITY, COMBAT ILLEGAL ACTIVITIES (MONEY LAUNDERING, TERRORISM FINANCING)
VERIFICATION METHODS	DOCUMENT VERIFICATION (ID SCANS, PROOF OF ADDRESS) BACKGROUND CHECKS INFORMATION CROSS-CHECKS AGAINST THIRD-PARTY DATABASES
AGE RESTRICTIONS	MINIMUM AGE REQUIREMENTS TO USE FINANCIAL SERVICES (PROTECTS MINORS)
SANCTIONS LISTS	VERIFYING AGAINST GOVERNMENT LISTS OF RESTRICTED INDIVIDUALS/ENTITIES
LEGAL CONSEQUENCES OF INADEQUATE VERIFICATION	<ul style="list-style-type: none">• FINANCIAL LOSSES (FRAUD, MONEY LAUNDERING)• REGULATORY PENALTIES (FINES, LICENSE SUSPENSIONS, CRIMINAL CHARGES)



AUTHENTICATION

FINANCE

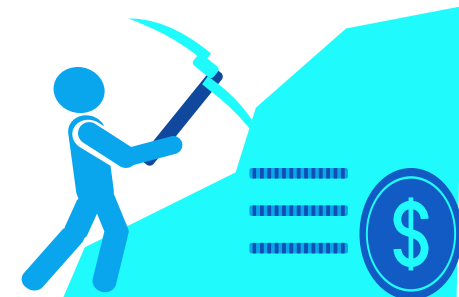
- Ensuring that the party attempting a transaction is who they claim to be.
- Protecting financial assets and preventing unauthorized access.

DIGITAL

- Implementing password systems, multi-factor authentication (MFA), and digital tokens for secure logins.
- Utilizing risk-based authentication protocols based on transaction type and user behavior.

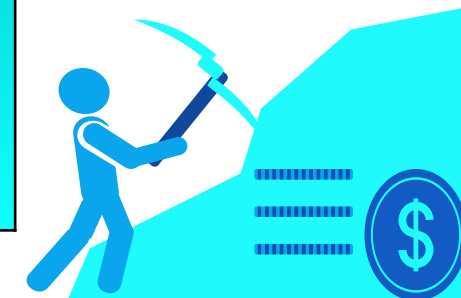
LAW

- Legal enforceability of digital authentication methods, such as electronic signatures and digital certificates.
- Liability associated with unauthorized access resulting from weak authentication procedures.
- Electronic signature laws governing the validity and legal effect of digital signatures.



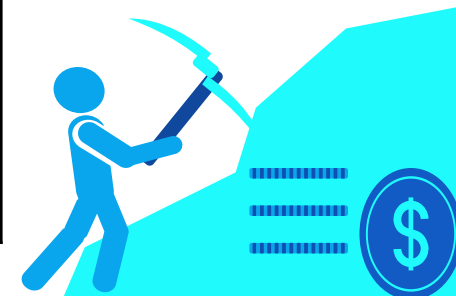
AUTHENTICATION - FINANCE

Aspect	Description
Goal	Ensuring that the party attempting a transaction is who they claim to be and protecting financial assets from unauthorized access.
Methods	Implementing password systems Multi-factor authentication (MFA) Digital tokens for secure logins Utilizing risk-based authentication protocols based on transaction type and user behavior.
Benefits	Prevents unauthorized access to accounts and financial information. Reduces fraud and financial losses. Increases customer trust and confidence in online financial services. Enables compliance with regulations like Know Your Customer (KYC)



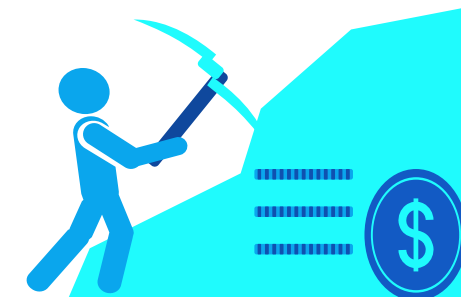
AUTHENTICATION – DIGITAL

Aspect	Description
Goal	Securing access to online resources and preventing unauthorized use of accounts and data.
Methods	Implementing password systems Multi-factor authentication (MFA) Digital tokens for secure logins
Benefits	Protects user accounts and data from unauthorized access. Enables secure access to online services like email, social media, and cloud storage. Improves overall security posture of digital systems.



AUTHENTICATION – LAW

Aspect	Description
Goal	Establishing the legal validity and enforceability of digital transactions and documents.
Methods	Legal enforceability of digital authentication methods (electronic signatures and digital certificates). Electronic signature laws governing the validity and legal effect of digital signatures.
Considerations	Liability associated with unauthorized access resulting from weak authentication procedures. Ensuring the authenticity and integrity of electronically signed documents. Compliance with relevant legal and regulatory requirements.



VERIFICATION VS. AUTHENTICATION

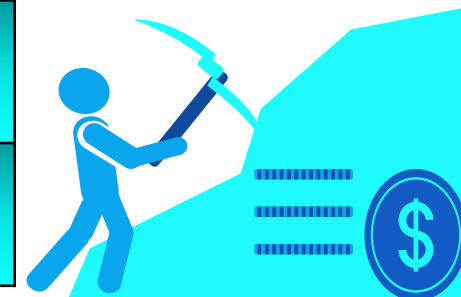


ASPECT	VERIFICATION	AUTHENTICATION
GOAL	CONFIRMS THE ACCURACY OF INFORMATION PROVIDED.	ENSURES THE PERSON INTERACTING WITH A SYSTEM IS WHO THEY CLAIM TO BE.
FOCUS	WHAT IS PRESENTED (INFORMATION)	WHO IS PRESENTING (IDENTITY)
PROCESS	CHECKING INFORMATION AGAINST A TRUSTED SOURCE (E.G., DATABASE, DOCUMENT)	VERIFYING THE USER'S CLAIMED IDENTITY THROUGH VARIOUS METHODS (E.G., PASSWORD, BIOMETRICS)
EXAMPLE	VERIFYING A DOCUMENT'S AUTHENTICITY (E.G., PASSPORT)	VERIFYING A USER'S IDENTITY WHEN LOGGING INTO A BANK ACCOUNT (E.G., PASSWORD + FINGERPRINT)
FREQUENCY	CAN BE A ONE-TIME PROCESS (E.G., VERIFYING A NEW ADDRESS)	OFTEN OCCURS MULTIPLE TIMES (E.G., LOGGING INTO DIFFERENT SYSTEMS)
ANALOGY	CHECKING IF A DOCUMENT IS A REAL COPY	CHECKING IF THE PERSON HOLDING THE DOCUMENT IS THE RIGHTFUL OWNER.

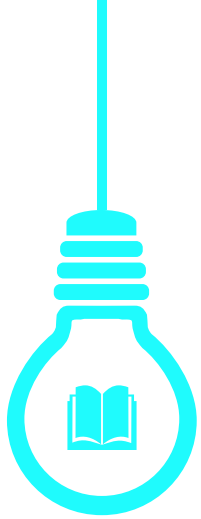


VERIFICATION VS. AUTHENTICATION

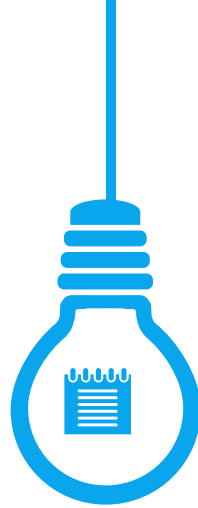
FEATURE	IDENTITY	VERIFICATION
WHAT IS PRESENTED?	INFORMATION PRESENTED (E.G., DOCUMENT, USERNAME)	-
WHO IS PRESENTING?	-	PERSON INTERACTING WITH A SYSTEM
OUTCOME	ESTABLISHES WHAT SOMETHING CLAIMS TO BE	CONFIRMS ACCURACY OF PRESENTED INFORMATION
METHOD	N/A	CHECKING INFORMATION AGAINST TRUSTED SOURCE (E.G., DATABASE)
EXAMPLE	PASSPORT	VERIFYING A PASSPORT AGAINST A GOVERNMENT DATABASE
FREQUENCY	VARIES (DEPENDS ON THE INFORMATION)	CAN BE ONE-TIME PROCESS (E.G., VERIFYING NEW ADDRESS)
FOCUS	UNDERSTANDING THE NATURE OF THE INFORMATION	CHECKING IF INFORMATION IS GENUINE



LEGAL PERSONHOOD



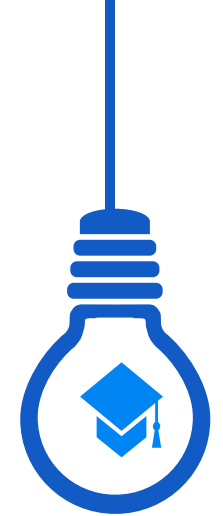
IS A STATUS THAT INDICATES THE RECOGNITION OF A LEGAL ENTITY AND ITS ABILITY TO HAVE CERTAIN RIGHTS AND OBLIGATIONS.



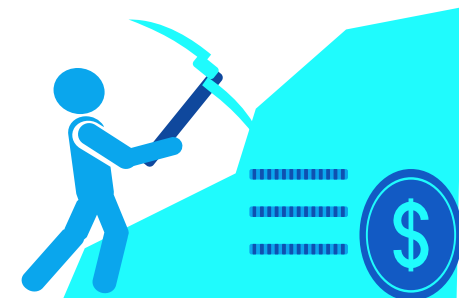
ENTITIES WITH SOME ESSENTIAL APTITUDES ARE AWARDED LEGAL PERSONHOOD UNDER THE CONSEQUENCE OF THESE CAPABILITIES.



AS A RESULT OF HAVING LEGAL PERSONHOOD, THESE ENTITIES CAN EXERCISE SOME RIGHTS AND ENTER INTO OBLIGATIONS.



IN TERMS OF HUMAN BEINGS, DUE TO THE PRESUMPTION OF HAVING PARTICULAR ABILITIES, PEOPLE ARE CONSIDERED NATURAL PERSONS.



الشخصية القانونية

هو وضع يدل على اعتراف الكيان القانوني بقدرته على امتلاك حقوق والتزامات معينة.



يعتبر البشر أشخاصاً طبيعيين بسبب افتراض امتلاكهم لقدرات محددة.



يتم منح الشخصية القانونية للكيانات التي تمتلك قدرات أساسية معينة نتيجة لهذه القدرات.

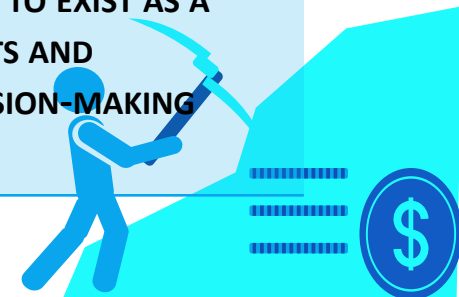


يمكن للكيانات ممارسة بعض الحقوق والدخول في التزامات بسبب امتلاكها الشخصية القانونية.



LEGAL CAPACITY Vs. PERSONAL LEGAL HOOD

FEATURE	LEGAL CAPACITY	PERSONAL LEGAL HOOD
DEFINITION	ABILITY TO UNDERSTAND AND MAKE LEGALLY BINDING DECISIONS	RECOGNITION AS A LEGAL PERSON WITH FUNDAMENTAL RIGHTS AND PROTECTIONS
SCOPE	VARIABLES DEPENDING ON AGE, MENTAL CAPACITY, AND LEGAL CONTEXT	BROADER CONCEPT ENCOMPASSING INHERENT RIGHTS
FOCUS	DECISION-MAKING ABILITY	RECOGNITION OF FUNDAMENTAL RIGHTS
EXAMPLES	CHILDREN HAVE LIMITED LEGAL CAPACITY DUE TO AGE, ADULTS WITH MENTAL IMPAIRMENTS MAY HAVE RESTRICTED LEGAL CAPACITY IN SPECIFIC AREAS	HUMANS, CORPORATIONS (IN SOME JURISDICTIONS) HAVE PERSONAL LEGAL HOOD
IMPLICATIONS	DETERMINES THE EXTENT TO WHICH AN INDIVIDUAL CAN EXERCISE THEIR RIGHTS AND MAKE LEGALLY BINDING DECISIONS	SIGNIFIES THE FUNDAMENTAL RIGHT TO EXIST AS A LEGAL ENTITY WITH INHERENT RIGHTS AND PROTECTIONS, REGARDLESS OF DECISION-MAKING CAPACITY

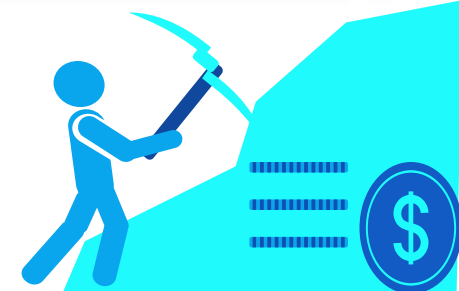


WHY CURRENT LEGAL FRAMEWORKS ARE UNSUITABLE FOR AI?

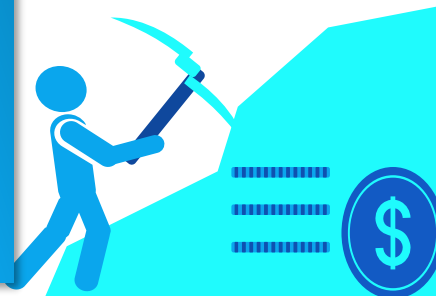
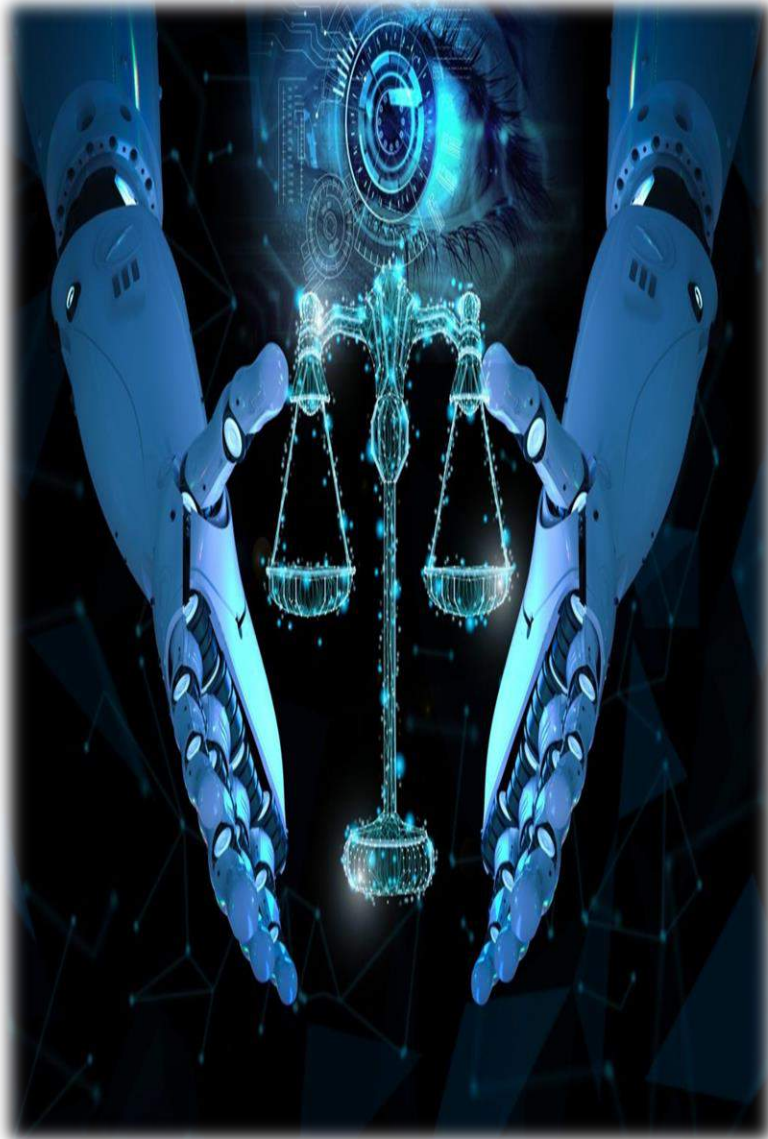
**JUDICIAL INTERPRETATIONS
WITHIN THE HUMAN CONTEXT**

HUMAN-CENTRIC FOCUS

**CODIFICATION BASED ON
HUMAN EXPERIENCE**



LEGAL PERSONHOOD CRITERIA



POSSIBLE LEGAL STATUS OF FUTURE AI



LACKING CRITICAL CAPABILITIES LIKE FREE WILL, EMPATHY, AND INTENTION, CURRENT AI CANNOT QUALIFY FOR LEGAL PERSONHOOD.



REGISTERING AI ENTITIES COULD REPRESENT ACCEPTANCE AS LEGAL SUBJECTS.

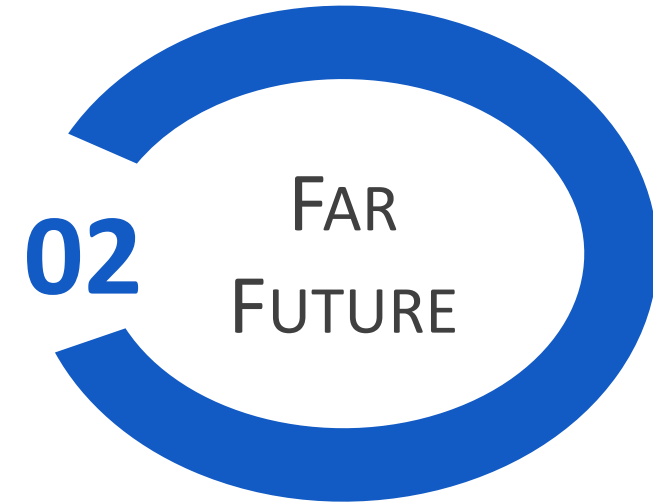
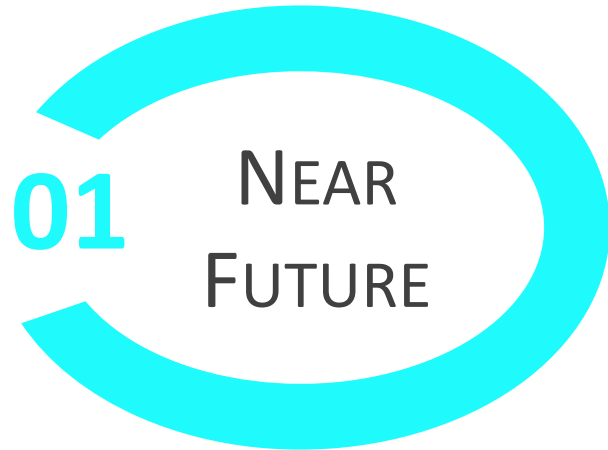


ELECTRONIC PERSONHOOD FOR ADVANCED AI SYSTEMS MIGHT EXIST SYMBOLICALLY WITHOUT IMPACTING CRIMINAL LAW.



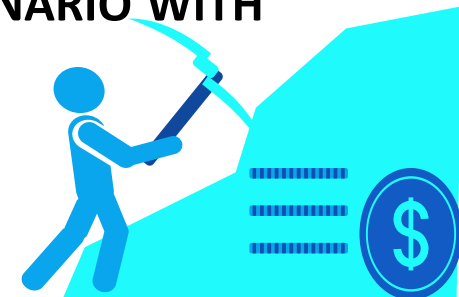
HUMANOID ROBOTS LIKE SOPHIA DON'T HAVE LEGAL PERSONHOOD; THEIR CITIZENSHIP WAS SYMBOLIC.

FUTURE SCENARIOS



- **DETERMINER TEST CAN ASSESS CAPABILITIES AND DETERMINE E-PERSONHOOD OR REGISTRATION.**
- **ACCEPTANCE AND USAGE IN SOCIETY WILL INFLUENCE LEGAL RECOGNITION.**
- **NON-HUMANOID AI SHOULDN'T BE DISADVANTAGED DUE TO APPEARANCE.**
- **DRIVERLESS CARS WILL BE A KEY EXAMPLE FOR LEGAL DISCUSSIONS.**

- **ADVANCED AI WITH COMPLEX DECISION-MAKING, EMOTIONS, OR SELF-AWARENESS MAY EMERGE.**
- **SCENARIOS RANGE FROM UTOPIAN TO DYSTOPIAN.**
- **FOCUS ON A PEACEFUL SCENARIO WITH ADVANCED HUMANOIDS.**



RELATIONSHIP BETWEEN LEGAL PERSONHOOD AND LEGAL CAPACITY TO ACT



LEGAL PERSONHOOD IS A PREREQUISITE FOR LEGAL CAPACITY. AN ENTITY CANNOT HAVE LEGAL CAPACITY WITHOUT FIRST BEING RECOGNIZED AS A LEGAL PERSON WITH RIGHTS AND OBLIGATIONS.



CHANGES IN LEGAL PERSONHOOD CAN AFFECT LEGAL CAPACITY. A MINOR GAINING LEGAL ADULTHOOD ACQUIRES FULL LEGAL CAPACITY, WHILE A CORPORATION UNDERGOING LIQUIDATION MIGHT LOSE ITS CAPACITY TO ENGAGE IN CERTAIN ACTIVITIES.



A NON-PROFIT ORGANIZATION WITH LEGAL PERSONHOOD MIGHT BE LIMITED IN ITS LEGAL CAPACITY TO SPECIFIC CHARITABLE ACTIVITIES OUTLINED IN ITS GOVERNING DOCUMENTS. IT MIGHT NOT BE ABLE TO ENGAGE IN COMMERCIAL VENTURES OUTSIDE ITS DEFINED CHARITABLE PURPOSE.

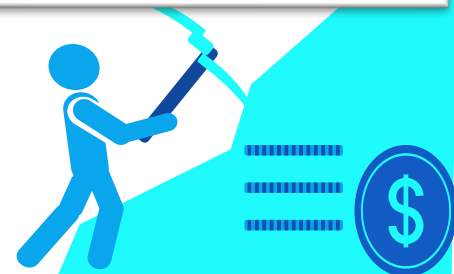


A CORPORATION, WHILE A LEGAL PERSON WITH THE CAPACITY TO CONDUCT BUSINESS, CANNOT VOTE IN ELECTIONS OR HOLD A PASSPORT, AS THESE RIGHTS AND OBLIGATIONS ARE TYPICALLY LIMITED TO INDIVIDUAL HUMAN BEINGS

وَعَلَّمَ آدَمَ الْأَسْمَاءَ كُلَّهَا ثُمَّ عَرَضَهُمْ عَلَى الْمَلَائِكَةِ
فَقَالَ أَنْبِئُونِي بِأَسْمَاءِ هَؤُلَاءِ إِنْ كُنْتُمْ صَادِقِينَ ﴿٣١﴾

قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ ﴿٣٢﴾

قَالَ يَا آدَمُ أَنْبِئْهُمْ بِأَسْمَائِهِمْ فَلَمَّا أَنْبَأَهُمْ بِأَسْمَائِهِمْ قَالَ
أَلَمْ أَقُلْ لَكُمْ إِنِّي أَعْلَمُ الْغَيْبَ السَّمَوَاتِ وَالْأَرْضِ وَأَعْلَمُ مَا
تُبْدُونَ وَمَا كُنْتُمْ تَكْتُمُونَ ﴿٣٣﴾

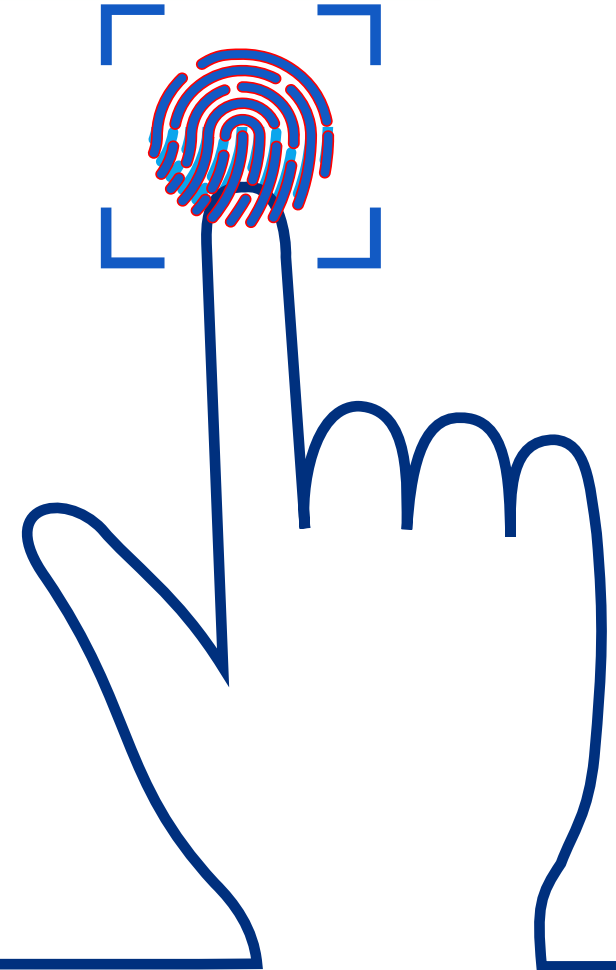


LEGAL CAPACITY TO ACT

- REFERS TO A PERSON'S ABILITY TO PERFORM LEGAL ACTS AND ENTER INTO CONTRACTS.
- IT INVOLVES THE UNDERSTANDING OF THE NATURE AND CONSEQUENCES OF ONE'S ACTIONS AND THE ABILITY TO GIVE INFORMED CONSENT.
- A PERSON WITH FULL LEGAL CAPACITY TO ACT IS GENERALLY CONSIDERED COMPETENT TO MAKE DECISIONS AND BE BOUND BY THEM.
- SOME INDIVIDUALS MAY HAVE LIMITED CAPACITY DUE TO AGE, MENTAL IMPAIRMENT, OR OTHER FACTORS. IN SUCH CASES, THEIR CAPACITY TO ACT MAY BE RESTRICTED OR SUBJECT TO CERTAIN SAFEGUARDS AND LEGAL PROTECTIONS.



KEY ASPECTS RELATED TO CAPACITY TO ACT IN BANKS



01

Age

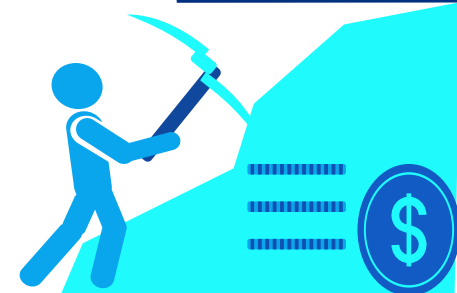
02

Mental Competence

03

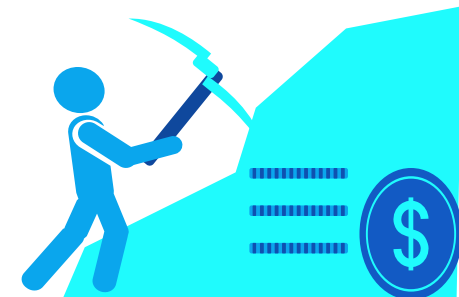
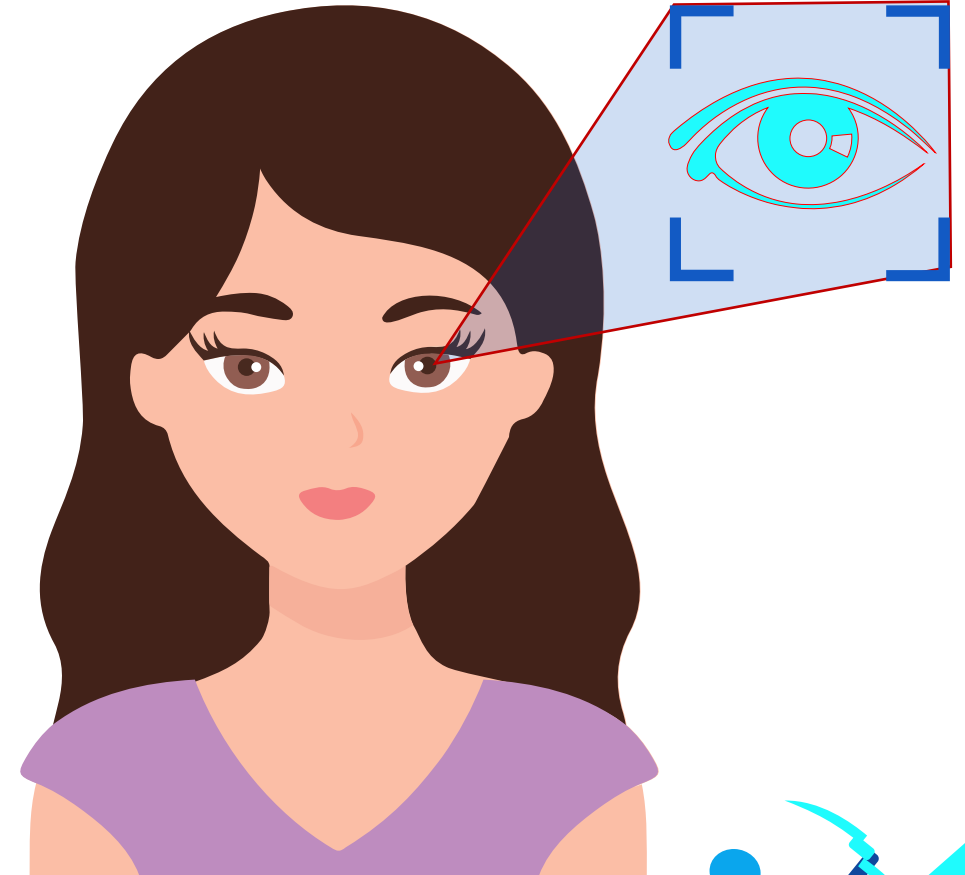
Legal Authority

Hint: IT IS ADVISABLE TO CONSULT WITH THE SPECIFIC BANK OR FINANCIAL INSTITUTION IN QUESTION TO DETERMINE THE EXACT CRITERIA FOR CAPACITY TO ACT IN BANKING MATTERS.



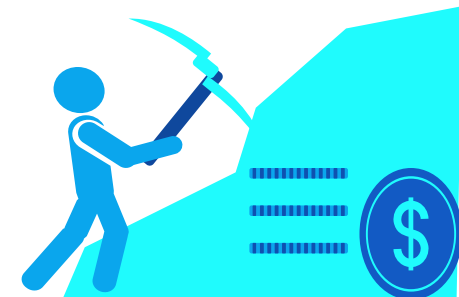
1- AGE

- **BANKS OFTEN HAVE MINIMUM AGE REQUIREMENTS FOR ACCOUNT HOLDERS.**
- **MINORS, INDIVIDUALS BELOW A CERTAIN AGE (TYPICALLY 18 YEARS OLD), MAY HAVE LIMITED CAPACITY TO ACT INDEPENDENTLY IN BANKING MATTERS.**
- **IN SUCH CASES, THEY MAY NEED A PARENT OR LEGAL GUARDIAN TO OPEN AND MANAGE THE ACCOUNT ON THEIR BEHALF.**



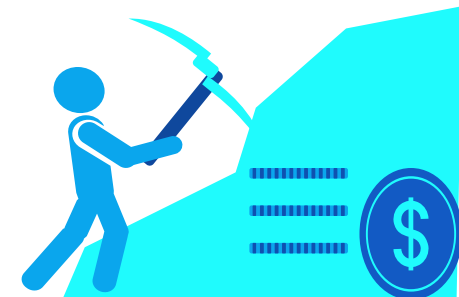
2- MENTAL COMPETENCE

- **BANKS OFTEN HAVE MINIMUM AGE REQUIREMENTS FOR ACCOUNT HOLDERS.**
- **MINORS, INDIVIDUALS BELOW A CERTAIN AGE MAY HAVE LIMITED CAPACITY TO ACT INDEPENDENTLY IN BANKING MATTERS.**
- **IN SUCH CASES, THEY MAY NEED A PARENT OR LEGAL GUARDIAN TO OPEN AND MANAGE THE ACCOUNT ON THEIR BEHALF.**



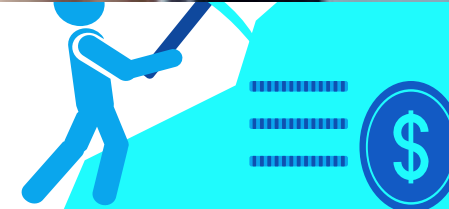
3- LEGAL AUTHORITY

- **IN CERTAIN CASES, INDIVIDUALS MAY ACT ON BEHALF OF OTHERS, SUCH AS POWER OF ATTORNEY, TRUSTEES, OR AUTHORIZED SIGNATORIES FOR BUSINESS ENTITIES**
- **IN SUCH INSTANCES, THEY MUST PROVIDE APPROPRIATE DOCUMENTATION TO PROVE THEIR LEGAL AUTHORITY TO ACT ON BEHALF OF THE ACCOUNT HOLDER.**



DIGITAL IDENTITY

- **PLAYS A CRUCIAL ROLE IN ONLINE SECURITY, PRIVACY, AND TRUST**
- **ENABLES INDIVIDUALS TO PROVE THEIR IDENTITY AND GAIN ACCESS TO DIGITAL SERVICES SECURELY**
- **RAISES CONCERNS REGARDING DATA PROTECTION, IDENTITY THEFT, AND PRIVACY RISKS**
- **VARIOUS TECHNOLOGICAL SOLUTIONS AND FRAMEWORKS ARE IMPLEMENTED TO ENSURE THE SECURE MANAGEMENT AND PROTECTION OF DIGITAL IDENTITIES, SUCH AS ENCRYPTION, MULTI-FACTOR AUTHENTICATION, AND IDENTITY MANAGEMENT SYSTEMS.**



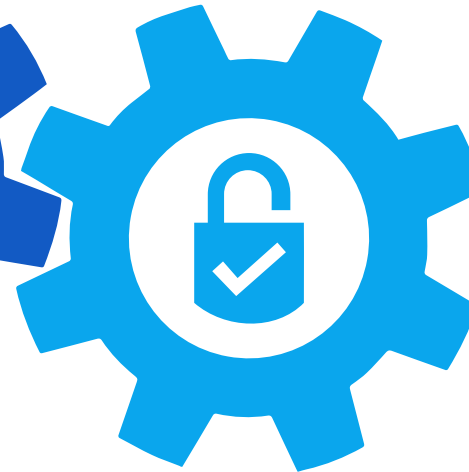
DIGITAL IDENTITY COMPONENTS



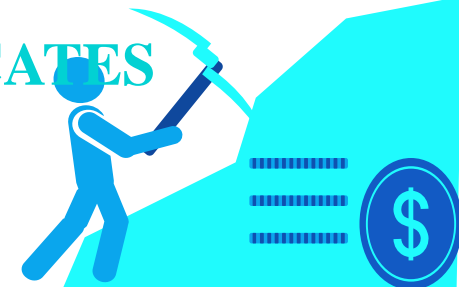
**IDENTITY
INFORMATION**



**AUTHORIZATIONS
AND PERMISSIONS**



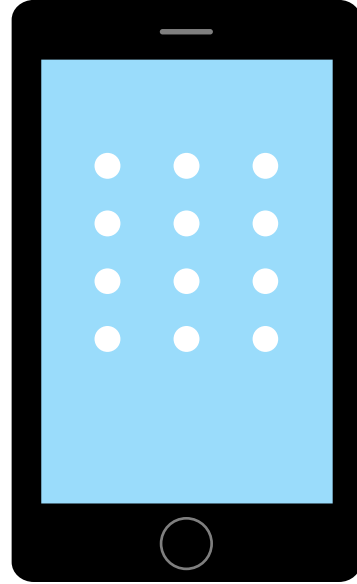
**AUTHENTICATION
CREDENTIALS / DIGITAL
CERTIFICATES**



IDENTITY RECOGNITION METHODS



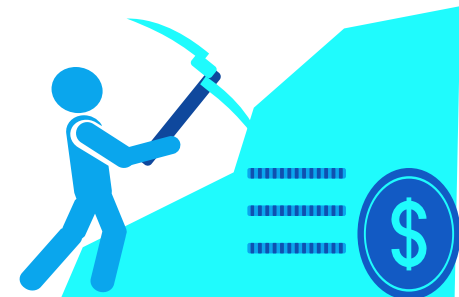
IDS



ATTESTATIONS /
CLAIMS

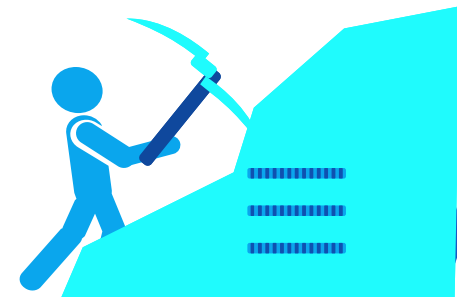


ATTRIBUTES



IDENTIFYING INDIVIDUALS: FOUR SOURCES AND THEIR APPLICATIONS

- IDENTIFICATION PLAYS A CRUCIAL ROLE IN VARIOUS ASPECTS OF OUR LIVES, FROM ACCESSING SERVICES TO ENSURING SECURITY.
- DETERMINING AN INDIVIDUAL'S IDENTITY OFTEN RELIES ON A COMBINATION OF FOUR KEY SOURCES:
 - DOCUMENTS
 - CLAIMS OF IDENTITY
 - ATTESTATION BY OTHERS
 - ATTRIBUTES



DOCUMENTS

EXPLANATION:

DOCUMENTS LIKE PASSPORTS, DRIVER'S LICENSES, NATIONAL IDENTIFICATION CARDS, AND BIRTH CERTIFICATES ARE OFFICIAL RECORDS CONTAINING PERSONAL INFORMATION THAT UNIQUELY IDENTIFIES AN INDIVIDUAL.

EXAMPLES:

- **A PASSPORT INCLUDES THE HOLDER'S NAME, PHOTOGRAPH, DATE OF BIRTH, NATIONALITY, AND PASSPORT NUMBER, PROVIDING STRONG IDENTIFICATION EVIDENCE.**
- **A DRIVER'S LICENSE VERIFIES THE INDIVIDUAL'S NAME, ADDRESS, PHOTOGRAPH, AND DRIVER'S LICENSE NUMBER.**

ADVISORIES:

- **DOCUMENTS SHOULD BE ISSUED BY RECOGNIZED AUTHORITIES AND PRESENT SECURITY FEATURES TO PREVENT FORGERY.**
- **BE CAUTIOUS OF TAMPERED OR ALTERED DOCUMENTS, AND VERIFY THEIR AUTHENTICITY THROUGH OFFICIAL CHANNELS IF POSSIBLE.**



CLAIMS OF IDENTITY

EXPLANATION:

AN INDIVIDUAL CLAIMING THEIR IDENTITY INVOLVES A DIRECT STATEMENT OF WHO THEY ARE. THIS CAN BE VERBAL OR WRITTEN, SUCH AS PROVIDING THEIR NAME, DATE OF BIRTH, OR OTHER PERSONAL DETAILS.

EXAMPLES:

- DURING A SECURITY CHECK AT AN AIRPORT, AN INDIVIDUAL PRESENTS THEIR PASSPORT AND VERBALLY CONFIRMS THEIR NAME AND DATE OF BIRTH.
- WHEN APPLYING FOR A JOB, A CANDIDATE SUBMITS THEIR RESUME WITH PERSONAL INFORMATION LIKE NAME, CONTACT DETAILS, AND EDUCATIONAL QUALIFICATIONS.

ADVISORIES:

- WHILE SELF-REPORTED INFORMATION CAN BE A STARTING POINT, IT REQUIRES VERIFICATION THROUGH OTHER SOURCES FOR RELIABLE IDENTIFICATION.
- BE AWARE OF POTENTIAL SITUATIONS WHERE INDIVIDUALS MIGHT INTENTIONALLY MISREPRESENT THEIR IDENTITY



ATTESTATION BY OTHERS

EXPLANATION:

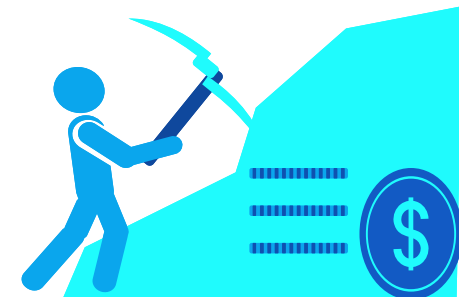
- **WITNESSING OR KNOWLEDGE FROM OTHERS CAN CONTRIBUTE TO IDENTIFYING AN INDIVIDUAL.**
- **THIS CAN INVOLVE STATEMENTS FROM ACQUAINTANCES, FAMILY MEMBERS, OR TRUSTED INDIVIDUALS WHO CAN VOUCH FOR THE PERSON'S IDENTITY.**

EXAMPLES:

- **IN A SMALL COMMUNITY, NEIGHBORS MIGHT RECOGNIZE A PERSON AND CONFIRM THEIR IDENTITY TO A NEWCOMER.**
- **DURING A LEGAL PROCEEDING, WITNESSES MIGHT TESTIFY TO KNOWING THE INDIVIDUAL AND THEIR TRUE IDENTITY.**

ADVISORIES:

- **THE RELIABILITY OF IDENTIFICATION THROUGH ATTESTATION DEPENDS ON THE CREDIBILITY AND KNOWLEDGE OF THE ATTESTING INDIVIDUALS.**
- **CONSIDER THE POTENTIAL FOR BIAS OR MANIPULATION WITHIN THE PROVIDED TESTIMONIES.**



ATTRIBUTES

EXPLANATION:

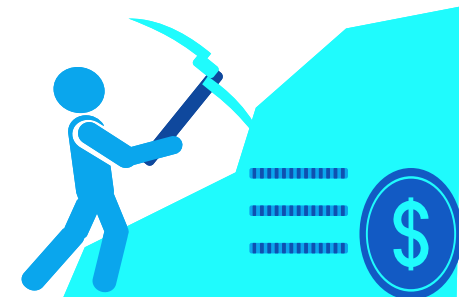
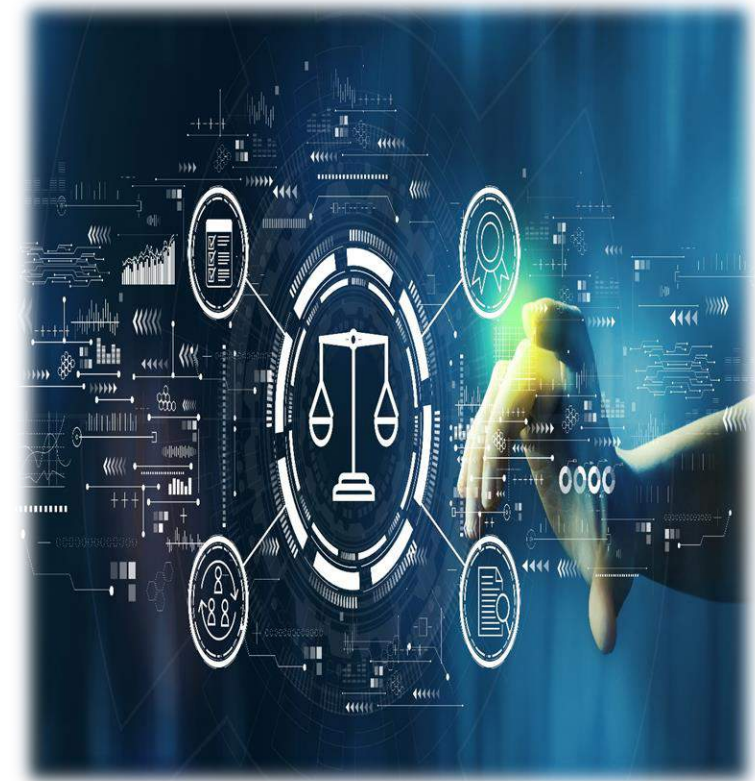
PHYSICAL ATTRIBUTES LIKE FACIAL FEATURES, FINGERPRINTS, DNA, OR EVEN VOICE PATTERNS CAN BE USED FOR IDENTIFICATION PURPOSES.

EXAMPLES:

- BIOMETRIC IDENTIFICATION SYSTEMS UTILIZE FINGERPRINTS, IRIS SCANS, OR FACIAL RECOGNITION TO VERIFY AN INDIVIDUAL'S IDENTITY.
- DNA TESTING CAN BE USED TO ESTABLISH BIOLOGICAL RELATIONSHIPS AND CONFIRM AN INDIVIDUAL'S IDENTITY IN SPECIFIC SITUATIONS.

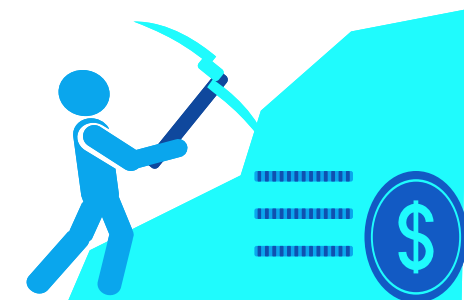
ADVISORIES:

- WHILE BIOMETRIC TECHNOLOGIES OFFER STRONG IDENTIFICATION POTENTIAL, DATA PRIVACY AND SECURITY CONCERNS NEED CAREFUL CONSIDERATION.
- THE ACCURACY AND RELIABILITY OF ATTRIBUTE-BASED IDENTIFICATION CAN VARY DEPENDING ON THE SPECIFIC TECHNOLOGY AND ITS IMPLEMENTATION.



COMBINING IDENTITY SOURCES FOR STRONGER IDENTIFICATION

- **NO SINGLE SOURCE IS FOOLPROOF, AND RELYING SOLELY ON ONE CAN LEAD TO ERRORS OR VULNERABILITIES.**
- **A ROBUST IDENTIFICATION PROCESS OFTEN INVOLVES A COMBINATION OF THESE SOURCES, CREATING A MORE COMPREHENSIVE AND RELIABLE PICTURE:**
 - **PRESENTING A VALID GOVERNMENT-ISSUED ID (DOCUMENT) ALONG WITH VERBAL CONFIRMATION OF IDENTITY (CLAIM).**
 - **UTILIZING BIOMETRIC VERIFICATION SYSTEMS (ATTRIBUTES) IN CONJUNCTION WITH DOCUMENT CHECKS.**
 - **CORROBORATING SELF-REPORTED INFORMATION (CLAIMS) WITH TESTIMONIES FROM TRUSTED INDIVIDUALS (ATTESTATION).**





DOCUMENTS - (CONTRACTS BETWEEN REMOTE[ABSENT] PARTIES)

EXPLANATION:

- IN THE DIGITAL REALM, SCANNED COPIES OF DOCUMENTS LIKE PASSPORTS, DRIVER'S LICENSES, OR NATIONAL IDENTIFICATION CARDS CAN SERVE AS IDENTIFICATION TOOLS.

EXAMPLES:

- WHEN OPENING AN ONLINE BANK ACCOUNT, SUBMITTING SCANNED COPIES OF GOVERNMENT-ISSUED IDs FOR VERIFICATION IS A COMMON PRACTICE.
- SECURE GOVERNMENT WEBSITES OR ONLINE PLATFORMS MIGHT UTILIZE DIGITAL CERTIFICATES TO ENSURE THE AUTHENTICITY OF THE PARTIES INVOLVED IN A CONTRACT.

ADVISORIES:

- SCRUTINIZE THE QUALITY AND AUTHENTICITY OF SCANNED DOCUMENTS, SEEKING VERIFICATION FROM OFFICIAL SOURCES IF NECESSARY.



CLAIMS OF IDENTITY - (CONTRACTS BETWEEN ABSENT PARTIES)

- **EXPLANATION:**

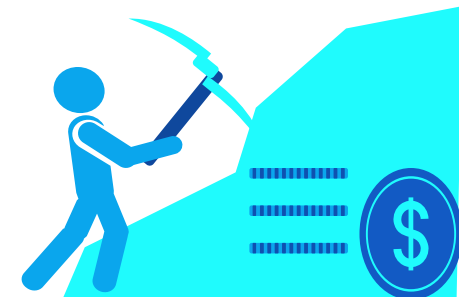
- IN DIGITAL INTERACTIONS, INDIVIDUALS OFTEN ESTABLISH THEIR IDENTITY THROUGH ONLINE PROFILES, EMAIL ADDRESSES, OR OTHER FORMS OF SELF-REPRESENTATION.

- **EXAMPLES:**

- WHEN ENTERING INTO A CONTRACT THROUGH AN ONLINE MARKETPLACE, BOTH PARTIES MIGHT RELY ON THEIR USER PROFILES OR EMAIL ADDRESSES FOR IDENTIFICATION.

- **ADVISORIES:**

- EXERCISE CAUTION WHEN SOLELY RELYING ON SELF-DECLARED IDENTITIES ONLINE.



ATTESTATION BY OTHERS - (CONTRACTS BETWEEN ABSENT PARTIES)

EXPLANATION:

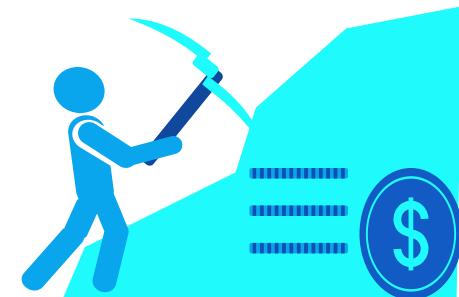
- IN THE DIGITAL REALM, ESTABLISHING TRUST THROUGH REPUTABLE THIRD-PARTY SERVICES CAN SERVE AS A FORM OF ATTESTATION.

EXAMPLES:

- PLATFORMS LEVERAGE THIRD-PARTY VERIFICATION SYSTEMS TO ASSESS THE CREDIBILITY OF FREELANCERS OR SERVICE PROVIDERS.

ADVISORIES:

- EVALUATE THE RELIABILITY AND REPUTATION OF THE THIRD-PARTY SERVICES PROVIDING ATTESTATION.
- UNDERSTAND THE LIMITATIONS AND GUARANTEES ASSOCIATED WITH THEIR VERIFICATION PROCESSES



DIGITAL ATTRIBUTES - (CONTRACTS BETWEEN ABSENT PARTIES)



EXPLANATION:

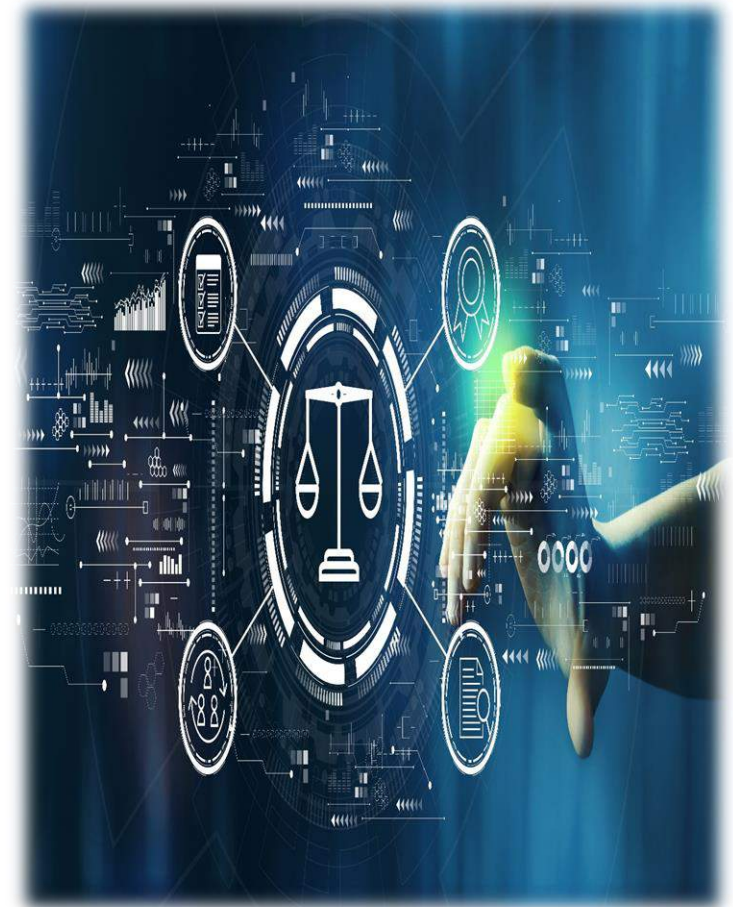
- BIOMETRIC TECHNOLOGIES LIKE FACIAL RECOGNITION OR FINGERPRINT SCANNERS ARE INCREASINGLY UTILIZED FOR DIGITAL IDENTITY VERIFICATION.

EXAMPLES:

- CERTAIN ONLINE BANKING APPS OR MOBILE PAYMENT SYSTEMS MIGHT UTILIZE FACIAL RECOGNITION.
- SPECIALIZED SOFTWARE CAN ANALYZE USER BEHAVIOR PATTERNS DURING ONLINE INTERACTIONS TO DETECT POTENTIAL FRAUD ATTEMPTS.

ADVISORIES:

- CONSIDER THE PRIVACY IMPLICATIONS OF BIOMETRIC DATA COLLECTION AND STORAGE.
- BE AWARE OF THE POTENTIAL LIMITATIONS AND ERROR RATES ASSOCIATED WITH BIOMETRIC IDENTIFICATION TECHNOLOGIES.



EKYC (ELECTRONIC KNOW YOUR CUSTOMER) - DOCUMENTS



METHOD:

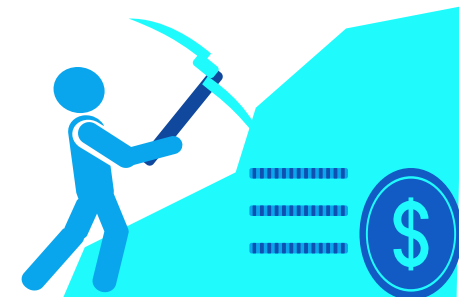
FINANCIAL INSTITUTIONS (FIs) CAN REQUEST SCANS OR DIGITAL COPIES OF OFFICIAL DOCUMENTS LIKE PASSPORTS, DRIVER'S LICENSES, OR NATIONAL IDs ISSUED BY TRUSTED GOVERNMENT BODIES.

EXAMPLE:

A FINTECH APP MIGHT ASK USERS TO UPLOAD PICTURES OF THEIR ID DURING ACCOUNT CREATION.

FINTECH/REG-TECH ROLE:

FINTECH CAN FACILITATE DOCUMENT CAPTURE THROUGH THEIR APPS, WHILE REG-TECH SOLUTIONS MIGHT VERIFY DOCUMENT AUTHENTICITY THROUGH INTEGRATIONS WITH GOVERNMENT DATABASES



EKYC (ELECTRONIC KNOW YOUR CUSTOMER) - CLAIMS

METHOD:

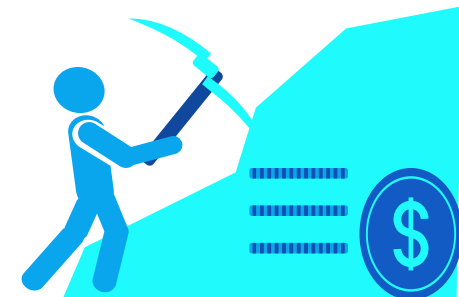
USERS PROVIDE INFORMATION ABOUT THEMSELVES, SUCH AS NAME, DATE OF BIRTH, ADDRESS, AND CONTACT DETAILS.

EXAMPLE:

WHILE REGISTERING FOR A MOBILE BANKING APP, USERS MIGHT BE ASKED TO FILL OUT A FORM WITH THEIR PERSONAL INFORMATION..

FINTECH/REG-TECH ROLE:

FINTECH PLATFORMS CAPTURE USER-PROVIDED CLAIMS, WHILE REGTECH SOLUTIONS CAN USE DATA ANALYTICS TO DETECT INCONSISTENCIES OR POTENTIAL FRAUD BASED ON THESE CLAIMS.



EKYC (ELECTRONIC KNOW YOUR CUSTOMER) - ATTESTATION



METHOD:

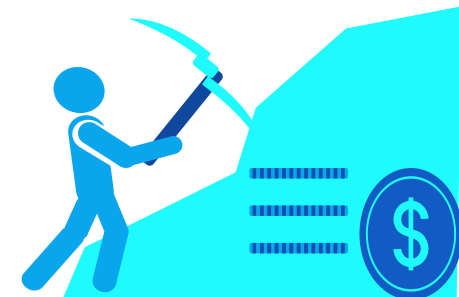
FIS CAN UTILIZE DATA FROM TRUSTED THIRD-PARTY SOURCES LIKE CREDIT BUREAUS, GOVERNMENT DATABASES, OR UTILITY COMPANIES TO VERIFY CLAIMS MADE BY USERS.

EXAMPLE:

A FINTECH LENDER MIGHT CONNECT TO CREDIT BUREAUS TO VERIFY A USER'S INCOME AND CREDITWORTHINESS DURING THE LOAN APPLICATION PROCESS.

FINTECH/REG-TECH ROLE:

FINTECH PLATFORMS CAN CONNECT TO VARIOUS DATA SOURCES FOR VERIFICATION, WHILE REG-TECH SOLUTIONS ENSURE SECURE DATA EXCHANGE AND COMPLIANCE WITH DATA PRIVACY REGULATIONS.



EKYC (ELECTRONIC KNOW YOUR CUSTOMER) - ATTRIBUTES

METHOD:

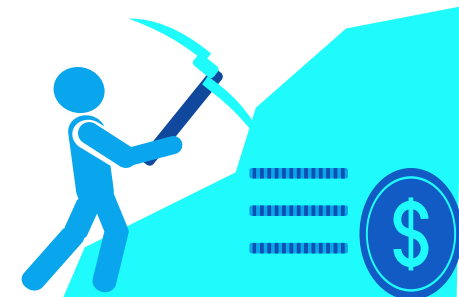
BIOMETRIC DATA (FINGERPRINTS, FACIAL RECOGNITION) OR DIGITAL SIGNATURES CAN BE USED FOR VERIFICATION, ESPECIALLY FOR HIGH-VALUE TRANSACTIONS.

EXAMPLE:

SOME MOBILE BANKING APPS MIGHT USE FINGERPRINT OR FACIAL RECOGNITION FOR LOGIN AND TRANSACTION APPROVALS.

FINTECH/REG-TECH ROLE:

FINTECH PLATFORMS CAN INTEGRATE BIOMETRIC AUTHENTICATION FEATURES, WHILE REG-TECH SOLUTIONS ENSURE SECURE STORAGE AND PROCESSING OF BIOMETRIC DATA.

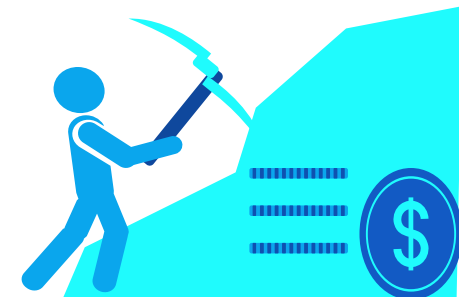


COMBINING IDENTITY SOURCES FOR SECURE DIGITAL CONTRACTS



A ROBUST IDENTIFICATION PROCESS FOR CONTRACTS BETWEEN ABSENT PARTIES IN THE DIGITAL DOMAIN OFTEN NECESSITATES A COMBINATION OF SOURCES:

- UTILIZING SCANNED DOCUMENTS OR DIGITAL CERTIFICATES FOR INITIAL VERIFICATION.
- EMPLOYING REPUTABLE THIRD-PARTY SERVICES TO PROVIDE ADDITIONAL LAYERS OF TRUST AND ATTESTATION.
- EXPLORING THE POTENTIAL OF BIOMETRIC TECHNOLOGIES WHERE APPROPRIATE, CONSIDERING THE ASSOCIATED PRIVACY CONCERNS AND LIMITATIONS.

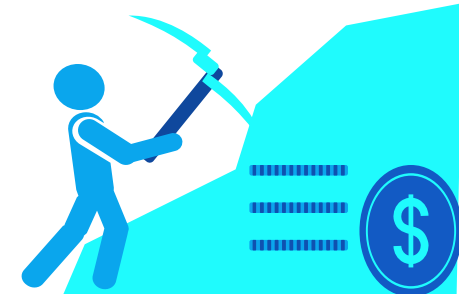


SOCIAL SELF THEORY BY GEORGE HERBERT MEAD

MEAD BELIEVED THAT OUR THOUGHTS, SELF-CONCEPT, AND THE WIDER COMMUNITY WE LIVE IN ARE CREATED THROUGH COMMUNICATION—SYMBOLIC INTERACTION.

SUGGESTS THAT ONLINE INTERACTIONS SHAPE IDENTITIES DIFFERENTLY, WITH USERS CULTIVATING AND ENHANCING PERSONAS IN THE DIGITAL REALM, PARTICULARLY IN ANONYMOUS SETTINGS LIKE SOCIAL MEDIA.

THE EVOLUTION OF DIGITAL TOOLS AND PLATFORMS ENABLES A DISTINCT DIGITAL HUMAN IDENTITY, SPARKING INTEREST IN EXPLORING THE DIFFERENCES BETWEEN DIGITAL AND REAL-WORLD IDENTITIES AND THE DEFINING CHARACTERISTICS OF EACH.



THE CONCEPT OF SYMBOLIC INTERACTIONISM BENEFITS

UNDERSTANDING THE FORMATION OF DIGITAL IDENTITIES:

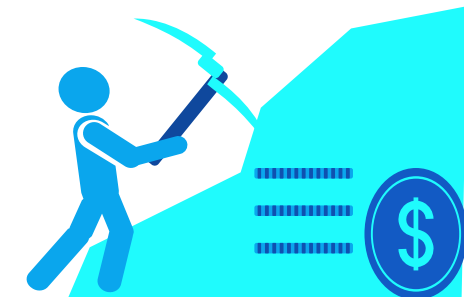
- PROVIDES A FRAMEWORK FOR UNDERSTANDING HOW ONLINE INTERACTIONS SHAPE OUR DIGITAL SELVES.
- HIGHLIGHTS THE ROLE OF COMMUNICATION (LANGUAGE, EMOJIS, ONLINE BEHAVIOR) IN CONSTRUCTING AND PRESENTING OUR ONLINE PERSONAS.

EXPLAINING THE UNIQUENESS OF DIGITAL IDENTITIES:

- RECOGNIZES THE DISTINCT NATURE OF DIGITAL IDENTITIES COMPARED TO REAL-WORLD IDENTITIES.
- ACKNOWLEDGES THE INCREASED FLUIDITY AND POTENTIAL FOR ANONYMITY IN ONLINE INTERACTIONS, ALLOWING FOR THE CULTIVATION OF DIFFERENT PERSONAS.

ANALYZING THE IMPACT OF ONLINE COMMUNITIES:

- EMPHASIZES THE INFLUENCE OF THE SPECIFIC ONLINE COMMUNITIES AND PLATFORMS ON HOW INDIVIDUALS PRESENT THEMSELVES DIGITALLY.
- HELPS US UNDERSTAND HOW THE NORMS AND EXPECTATIONS OF DIFFERENT ONLINE SPACES SHAPE DIGITAL IDENTITIES.



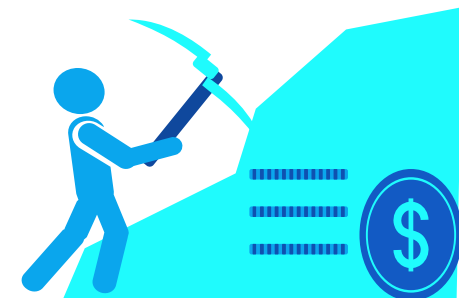
THE CONCEPT OF SYMBOLIC INTERACTIONISM BENEFITS

INFORMING RESPONSIBLE DIGITAL INTERACTION:

- BY RECOGNIZING THE CONSTRUCTED NATURE OF DIGITAL IDENTITIES, IT ENCOURAGES CRITICAL AWARENESS OF HOW WE PRESENT OURSELVES ONLINE.
- IT PROMOTES RESPONSIBLE ONLINE BEHAVIOR AND MINDFUL COMMUNICATION, CONSIDERING THE POTENTIAL IMPACT ON BOTH OUR OWN AND OTHERS' DIGITAL PERSONAS.

GUIDING DIGITAL IDENTITY DESIGN:

- THIS CONCEPT CAN BE APPLIED TO DESIGNING ONLINE PLATFORMS AND TOOLS THAT CONSIDER THE DYNAMIC NATURE OF DIGITAL IDENTITIES.
- IT CAN INFORM THE DEVELOPMENT OF FEATURES THAT SUPPORT POSITIVE AND AUTHENTIC ONLINE SELF-EXPRESSION WHILE ACKNOWLEDGING THE COMPLEXITIES OF THE DIGITAL REALM.



CHALLENGES - CONCEPT OF SYMBOLIC INTERACTIONISM

TO UNDERSTANDING DIGITAL IDENTITIES

DYNAMIC AND EVOLVING NATURE OF ONLINE INTERACTIONS:

- ONLINE INTERACTIONS ARE CONSTANTLY EVOLVING, WITH NEW PLATFORMS, TRENDS, AND COMMUNICATION STYLES EMERGING.
- KEEPING PACE WITH THIS DYNAMIC ENVIRONMENT CAN BE CHALLENGING WHEN ANALYZING THE FORMATION AND IMPACT OF DIGITAL IDENTITIES.

MEASURING AND QUANTIFYING ONLINE IDENTITY:

- SYMBOLIC INTERACTIONISM EMPHASIZES THE SUBJECTIVE AND CONSTRUCTED NATURE OF IDENTITY, MAKING IT DIFFICULT TO OBJECTIVELY MEASURE OR QUANTIFY DIGITAL PERSONAS.
- ASSESSING THE INFLUENCE OF ONLINE INTERACTIONS ON INDIVIDUALS' SELF-PERCEPTION AND OVERALL IDENTITY CAN BE COMPLEX.



CHALLENGES - CONCEPT OF SYMBOLIC INTERACTIONISM

TO UNDERSTANDING DIGITAL IDENTITIES

ETHICAL CONSIDERATIONS IN ONLINE RESEARCH:

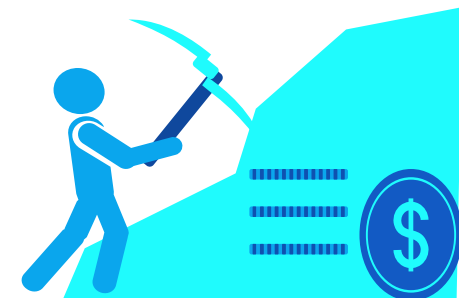
- STUDYING ONLINE BEHAVIOR RAISES ETHICAL CONCERNS REGARDING PRIVACY, DATA COLLECTION, AND INFORMED CONSENT.
- RESEARCHERS MUST ENSURE RESPONSIBLE DATA PRACTICES AND PROTECT THE PRIVACY OF INDIVIDUALS PARTICIPATING IN ONLINE INTERACTIONS.

POTENTIAL FOR MISREPRESENTATION AND DECEPTION:

- THE CONCEPT ACKNOWLEDGES THE POTENTIAL FOR INDIVIDUALS TO CULTIVATE DIFFERENT PERSONAS ONLINE, SOMETIMES INVOLVING MISREPRESENTATION OR DECEPTION.
- DISTINGUISHING BETWEEN GENUINE SELF-EXPRESSION AND FABRICATED ONLINE IDENTITIES CAN BE CHALLENGING.

CULTURAL AND CONTEXTUAL VARIATIONS:

- ONLINE COMMUNITIES AND PLATFORMS EXIST WITHIN DIVERSE CULTURAL CONTEXTS WITH VARYING NORMS AND EXPECTATIONS.
- UNDERSTANDING THE IMPACT OF THESE VARIATIONS ON THE FORMATION AND PRESENTATION OF DIGITAL IDENTITIES REQUIRES CAREFUL CONSIDERATION



LEGAL CAPACITY'S IMPACT ON DIGITAL IDENTIFICATION

**IDENTITY VERIFICATION, CHILD ONBOARDING, AND
LEGAL CAPACITY**

**AI AND TECHNOLOGY ADVANCEMENTS RAISE
LEGAL CAPACITY CONSIDERATIONS.**

**ONLINE ENVIRONMENTS, OR CYBERSPACE, HAVE
UNIQUE CHARACTERISTICS INFLUENCING IDENTITY
FORMATION, DISTINCT FROM THE REAL WORLD.**



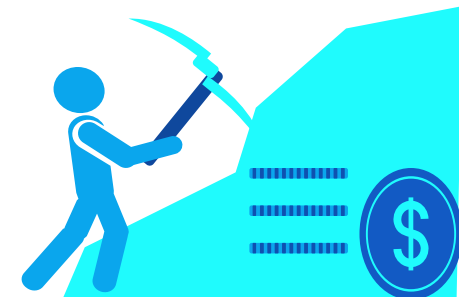
CHILD ONBOARDING - LEGAL CAPACITY CHALLENGES

AGE-VARYING LEGAL CAPACITY:

- CHILDREN'S LEGAL CAPACITY TO ENTER INTO CONTRACTS AND MAKE INDEPENDENT DECISIONS VARIES SIGNIFICANTLY DEPENDING ON THEIR AGE AND JURISDICTION.
- THIS CREATES A MOVING TARGET FOR PLATFORMS SEEKING TO ONBOARD THEM WHILE ENSURING LEGAL COMPLIANCE.

PARENTAL CONSENT:

- IN MOST JURISDICTIONS, PARENTAL CONSENT IS REQUIRED FOR CHILDREN TO ENGAGE IN ONLINE ACTIVITIES, ESPECIALLY THOSE INVOLVING FINANCIAL TRANSACTIONS OR DATA SHARING.
- THIS NECESSITATES ROBUST AGE VERIFICATION MECHANISMS AND CLEAR COMMUNICATION OF PARENTAL CONSENT REQUIREMENTS.



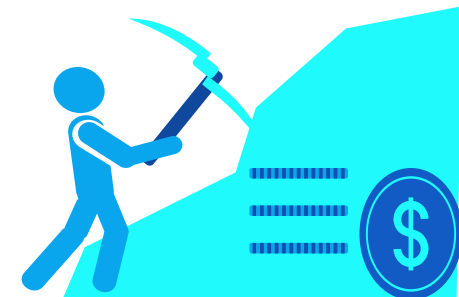
CHILD ONBOARDING - LEGAL CAPACITY CHALLENGES

DATA PRIVACY AND PROTECTION:

- CHILDREN'S DATA IS PARTICULARLY SENSITIVE AND REQUIRES HEIGHTENED PROTECTION UNDER LAWS LIKE COPPA (CHILDREN'S ONLINE PRIVACY PROTECTION ACT) IN THE US AND GDPR (GENERAL DATA PROTECTION REGULATION) IN THE EU.
- PLATFORMS MUST IMPLEMENT STRINGENT DATA SECURITY MEASURES AND OBTAIN PARENTAL CONSENT FOR DATA COLLECTION AND USAGE.

UNDERSTANDING TERMS OF SERVICE:

- COMPLEX LEGAL TERMS AND CONDITIONS CAN BE CHALLENGING FOR CHILDREN TO COMPREHEND.
- PLATFORMS MUST PRESENT INFORMATION IN A CHILD-FRIENDLY MANNER, ENSURING THEY UNDERSTAND THE IMPLICATIONS OF THEIR ACTIONS AND THE POTENTIAL RISKS INVOLVED.



CHILD ONBOARDING - SOLUTIONS AND CONSIDERATIONS

AGE-GATING:

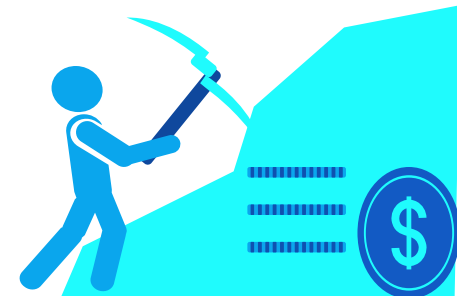
- IMPLEMENTING AGE VERIFICATION MECHANISMS THROUGH ID CHECKS OR PARENTAL VERIFICATION TOOLS IS CRUCIAL
- THIS TO ENSURE CHILDREN ARE NOT ACCESSING AGE-RESTRICTED CONTENT OR SERVICES.

PARENTAL CONTROLS:

- PROVIDING PARENTS WITH ROBUST PARENTAL CONTROL TOOLS.
- THIS ALLOWS THEM TO MONITOR THEIR CHILDREN'S ONLINE ACTIVITY, SET LIMITATIONS, AND MANAGE DATA SHARING PERMISSIONS.

SIMPLIFIED USER INTERFACES:

- DESIGNING USER INTERFACES THAT ARE CLEAR, CONCISE, AND VISUALLY APPEALING FOR CHILDREN IS ESSENTIAL
- THIS TO ENSURE THEY CAN NAVIGATE THE PLATFORM SAFELY AND UNDERSTAND THEIR OPTIONS.



CHILD ONBOARDING - SOLUTIONS AND CONSIDERATIONS

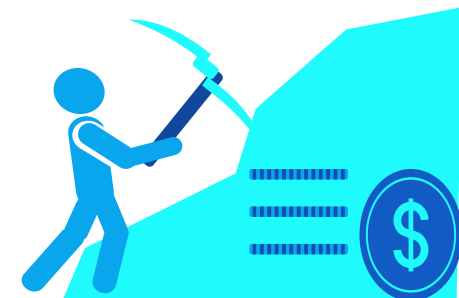


EDUCATIONAL RESOURCES:

- PROVIDING EDUCATIONAL RESOURCES AND AGE-APPROPRIATE EXPLANATIONS OF TERMS AND CONDITIONS.
- THIS CAN EMPOWER CHILDREN TO MAKE INFORMED DECISIONS WITHIN THEIR DEVELOPING LEGAL CAPACITY.

COLLABORATION WITH CHILD RIGHTS ORGANIZATIONS:

- PARTNERING WITH CHILD RIGHTS ORGANIZATIONS AND LEGAL EXPERTS
- THIS HELPS PLATFORMS STAY UPDATED ON EVOLVING REGULATIONS AND BEST PRACTICES FOR PROTECTING CHILDREN'S RIGHTS IN THE DIGIT



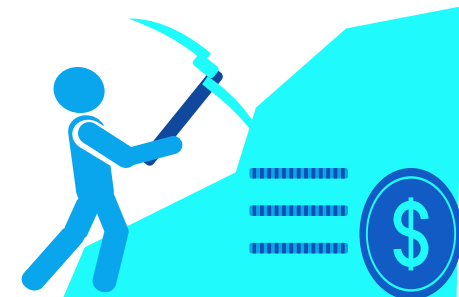
AI AND TECHNOLOGY ADVANCEMENTS RAISE LEGAL CAPACITY CONSIDERATIONS

EVOLVING AGE OF CONSENT

THE TRADITIONAL AGE OF CONSENT FOR ONLINE ACTIVITIES AND DATA COLLECTION MAY NEED TO BE RE-EVALUATED.

ALGORITHMIC BIAS AND DISCRIMINATION

- RAISES CONCERNS ABOUT THE LEGAL IMPLICATIONS OF ALGORITHMIC DECISIONS THAT MAY UNFAIRLY DISADVANTAGE INDIVIDUALS BASED ON FACTORS LIKE RACE, GENDER, OR SOCIOECONOMIC STATUS.
- DETERMINING LEGAL CAPACITY IN THE CONTEXT OF AI-DRIVEN DECISION-MAKING PROCESSES BECOMES COMPLEX, REQUIRING SAFEGUARDS AGAINST BIASED OUTCOMES AND POTENTIAL DISCRIMINATION.



LEGAL CONSIDERATIONS OF AI ADVANCEMENTS

AI AND TECHNOLOGY ADVANCEMENTS RAISE LEGAL CAPACITY CONSIDERATIONS

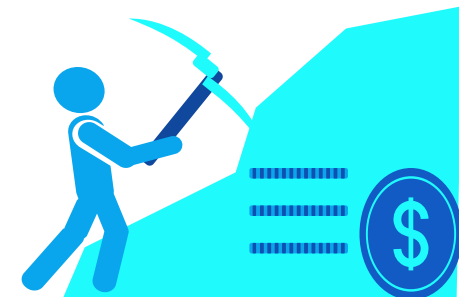
ATTRIBUTION OF RESPONSIBILITY IN AI-DRIVEN INTERACTIONS:

WHO IS RESPONSIBLE FOR THE ACTIONS AND DECISIONS OF AI SYSTEMS?

DATA PRIVACY AND INFORMED CONSENT:

HOW LEGAL FRAMEWORKS SHOULD ADAPT TO PROTECT INDIVIDUAL PRIVACY IN THE CONTEXT OF AI?

- **CLEAR AND ACCESSIBLE INFORMATION:** INDIVIDUALS, INCLUDING CHILDREN, SHOULD HAVE EASY-TO-UNDERSTAND INFORMATION ABOUT HOW THEIR DATA IS COLLECTED, USED, AND SHARED BY AI SYSTEMS.
- **CAPACITY FOR INFORMED CONSENT:** LEGAL FRAMEWORKS SHOULD ENSURE INDIVIDUALS HAVE THE ABILITY TO GIVE INFORMED CONSENT REGARDING THEIR DATA AND AI INTERACTIONS.

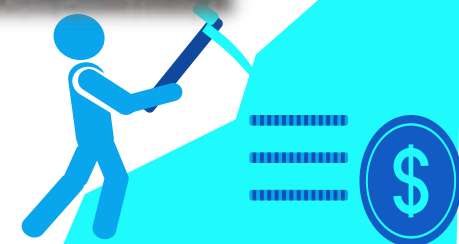
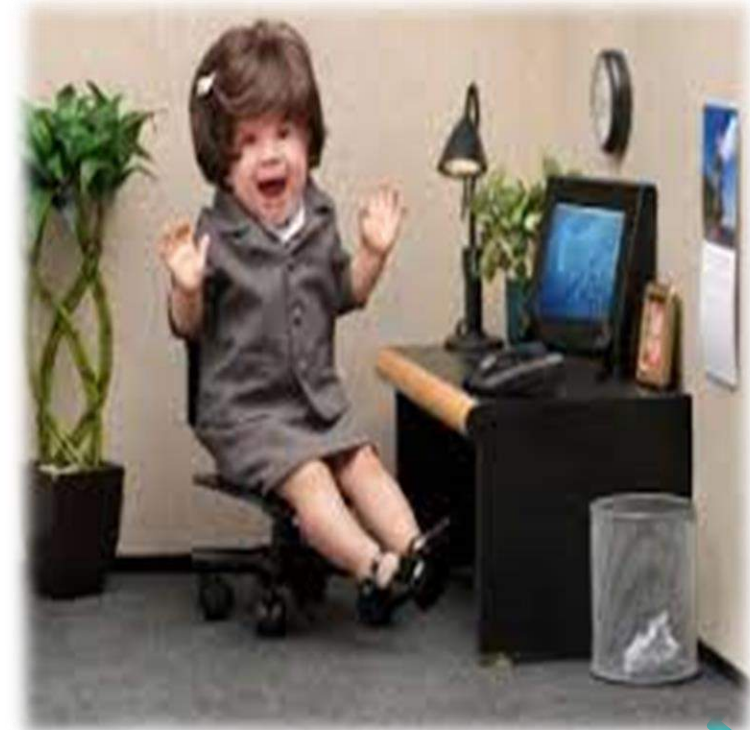


LEGAL ISSUES CONCERNING CHILD ONBOARDING

CHALLENGES IN CHILD ONBOARDING, PARTICULARLY CONCERNING OBTAINING CONSENT FROM LEGAL GUARDIANS AND COMPLYING WITH AGE-SPECIFIC REGULATIONS.

THE EU'S DIGITAL SERVICES ACT (DSA) AND FORTHCOMING CODE OF CONDUCT AIM TO HARMONIZE REGULATIONS AND ENSURE THE PRIVACY AND SECURITY OF CHILDREN USING DIGITAL SERVICES, THEY FOSTER COLLABORATION BETWEEN INDUSTRY, POLICYMAKERS, AND CIVIL SOCIETY.

EFFORTS ARE FOCUSED ON SUPPORTING AGE VERIFICATION METHODS THAT RESPECT PRIVACY AND SECURITY, ALIGNING WITH EMERGING REGULATIONS AND INTERNATIONAL STANDARDS TO PROVIDE DIVERSE OPTIONS FOR AGE ASSURANCE IN A GROWING ECOSYSTEM.



DIGITAL DIVIDE CAUSES AND IMPACT ON LEGAL CAPACITY

REFERS TO THE GAP BETWEEN INDIVIDUALS WHO HAVE ACCESS TO AND EFFECTIVELY USE INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTs) AND THOSE WHO DO NOT.

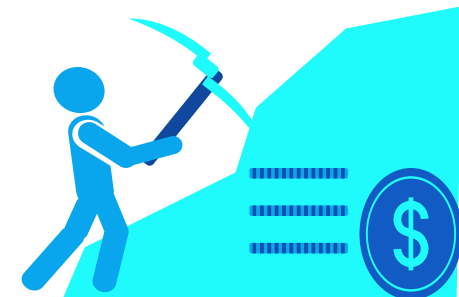
CAUSES

ECONOMIC DISPARITY:

LACK OF FINANCIAL RESOURCES CAN PREVENT INDIVIDUALS FROM AFFORDING DEVICES, INTERNET ACCESS, OR DATA PLANS.

GEOGRAPHIC LOCATION:

RURAL AREAS OFTEN HAVE LIMITED OR UNRELIABLE INTERNET INFRASTRUCTURE COMPARED TO URBAN AREAS.



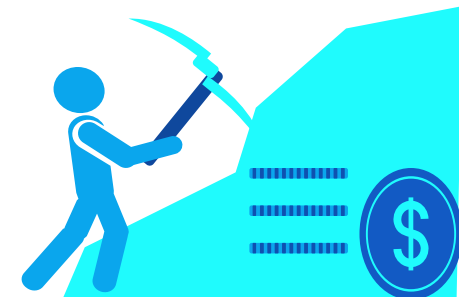
DIGITAL DIVIDE CAUSES AND IMPACT ON LEGAL CAPACITY

DIGITAL LITERACY:

LACK OF SKILLS OR KNOWLEDGE TO NAVIGATE TECHNOLOGY CAN HINDER INDIVIDUALS FROM FULLY UTILIZING ITS POTENTIAL.

IMPACT ON LEGAL CAPACITY:

WHEN AI-POWERED TOOLS AND TECHNOLOGIES BECOME INCREASINGLY INTEGRATED INTO LEGAL PROCESSES AND INTERACTIONS, INDIVIDUALS WITHOUT ADEQUATE ACCESS TO THEM FACE LIMITATIONS IN DEVELOPING THEIR LEGAL CAPACITY.



THANK YOU

