Technical report on Atala PRISM Modular KYC Solution by IAMX with ID 1100031
Milestone: 2

Project ID	1100031
Link full project	https://projectcatalyst.io/funds/11/cardano-use-cases-solution/atala-prism-modular-kyc-solution-by-iamx
Challenge	F11: Cardano Use Cases: Solution
Milestone 2	https://milestones.projectcatalyst.io/projects/1100031/milestones/2
Live-URL for testing	https://kyc.iamx.id/onboarding/atalaprism
GitHub Technical report	https://github.com/IAMXID/Atala-PRISM-Modular-KYC-Solution
GitHub Video	https://github.com/IAMXID/Atala-PRISM-Modular-KYC-Solution
Acceptance criteria	Acceptance criteria An individual has the ability to complete the text- and rules-based chatbot, including ID Verification, Liveness Check, Proof of Address, AML, Media Check and Enhanced Due Diligence, based on the following acceptance criteria: 1. Video Walkthrough Capture a video walkthrough of the entire process of interacting with the chatbot, ID Verification, Liveness Check, Proof of Address, AML, Media Check and Enhanced Due Diligence. This should include the start page, each step of interaction, and the completion or confirmation page that indicates the process has been successfully finished. 2. Technical Reports Provide technical reports that show the interaction data with the chatbot, ID Verification, Liveness Check, Proof of Address, AML, Media Check and Enhanced Due Diligence. This data is anonymized to protect personal information but will include timestamps, types of questions answered, and the completion status. 3. The chatbot, ID Verification, Liveness Check, Proof of Address, AML, Media Check and Enhanced Due Diligence are not open-source.
Evidence of milestone completion	1. Documentation of Video Walkthrough in GitHub (https://github.com/IAMXID/Atala-PRISM-Modular-KYC-Solution) for Chatbot, ID Verification, Liveness Check, Proof of Address, AML, Media Check and Enhanced Due Diligence 2. Documentation of technical reports in GitHub (https://github.com/IAMXID/Atala-PRISM-Modular-KYC-Solution) for Chatbot, ID Verification, Liveness Check, Proof of Address, AML, Media Check and Enhanced Due Diligence

The color green is used to point out evidence.

Table of Contents

1. About

- This technical report details the development and implementation of the Atala PRISM Modular KYC Solution by IAMX, with ID 1100031.

- The solution introduces a chatbot-based prototype designed to facilitate identity verification and management, leveraging Atala PRISM's infrastructure.

- This initiative aims to enable developers to craft and deploy compliant, reusable digital identities for a variety of real-world applications.

- The Atala PRISM Modular KYC Solution is divided into several modules, each designed to enhance different aspects of identity verification and compliance. The milestones 1-5 build sequentially on each other. Milestone 2 includes everything from Milestone 1 and the new functions of Milestone 2.

Table 1: Overview Elements and Functions included in Milestones 1-5 and Partners

Overview Elements and Functions included in Milestones 1-5 and Partners		
Milestone	**Element / Functions**	**Partner**
1	• Chatbot	IAMX
2	• ID-Verification Level 3 • Liveness & face match • Security features document • Address verification • AML (pep, sanction, crime) • Enhanced due diligence	IDnow Intrum
3	• KYT, transaction and wallet monitoring	Merkle Science
4	• creation of did:prism, creation of verifiable credential	IAMX
5	• Demo with 3 different individuals / nationalities	IAMX

2. Understanding KYC: Know Your Customer

KYC, or "Know Your Customer," is a fundamental process used by businesses, particularly in the financial sector, to verify the identity of their clients. This process involves several checks and measures designed to confirm the legitimacy of the customer's identity, assess potential risks, and ensure compliance with legal and regulatory requirements and is carried out in modular levels. The topic of KYC, AML require an understanding of the meaning, industries it refers to, legal sources, certification levels to be met, obligations and response actions in case of a match.

2.1 What KYC Includes

A full KYC process typically includes the following elements:

1. Identity Verification:
Collecting and verifying personal information such as name, address, date of birth, and national identification numbers (e.g., passport or driver's license).
Using biometric verification methods like facial recognition and liveness detection to ensure the person presenting the ID is physically present and matches the document.

2. Liveness & Face Match:
Employing advanced biometric technologies to confirm that the customer is a real, live person and that their facial features match the provided identification documents. This step is crucial to prevent identity fraud and spoofing attacks.

3. Document Verification:
Analyzing identification documents to ensure they are authentic and untampered. This involves checking for security features such as watermarks, holograms, and microprinting to verify the legitimacy of the documents.

4. Address Verification:
Verifying the customer's residential address through utility bills, bank statements, or direct verification with government databases. This helps ensure the accuracy of the address provided and mitigates the risk of fraudulent activities.

5. AML Screening:
Conducting Anti-Money Laundering (AML) checks to identify whether the customer appears on any sanctions lists, watchlists for politically exposed persons (PEPs), or databases of individuals with known criminal activities. This screening helps prevent money laundering and terrorist financing.

6. Enhanced Due Diligence (EDD):
Applying additional scrutiny to high-risk customers or transactions. This may include more comprehensive background checks, gathering more detailed customer information, and continuous monitoring of transactions to ensure ongoing compliance and risk management.

7. KYT (Know Your Transaction):
Continuously analyzing customer transactions to detect unusual or suspicious activities. This involves monitoring wallet and transaction activities to identify patterns that could indicate fraudulent behavior or financial crime, ensuring compliance with regulatory standards.

2.2 Goals and Intentions of KYC

1. Prevent Financial Crimes
By verifying identities and conducting background checks, KYC helps prevent money laundering, terrorist financing, fraud, and other financial crimes.

2. Ensure Regulatory Compliance
KYC helps businesses comply with local and international laws and regulations, which is critical to avoid legal penalties and maintain operating licenses.

3. Protect Businesses and Customers
By ensuring the legitimacy of customers, businesses can protect themselves and their customers from fraud and reputational damage.

4. Enhance Trust and Transparency
Effective KYC processes build trust between businesses and their customers by demonstrating a commitment to security and compliance.

2.3 Industries and products requiring KYC

KYC requirements are essential across various industries and for numerous products, ensuring compliance with regulatory standards and safeguarding against financial crimes. Here's a detailed overview of the industries and products where KYC is crucial:

Table 2: Industries and products requiring KYC

Banking and Financial Services	Insurance	Telecommunications	Cryptocurrency and Digital Assets
Bank accounts Loans Credit Cards Payment Services Financial Advisory Corporate Banking	Life Health Auto Home Travel Property Business Marine Disability Claims Processing	Prepaid Postpaid Fixed Line Internet Mobile Money Cable Sat TV VoIP	CEX DEX with compliance features Custodial wallets ICOs, STOs, IEOs DeFi securities, lending, liquidity, insurance Payment Gateways DAOs NFT marketplaces Crypto ATMs Custody Funds Stablecoins Savings

Fintech	Mobility	Gaming	Travel
Digital Banking Payment Services P2P Lending Robo Advisor Crowdfunding Stock Trading Investments Payment Apps Buy Now Pay Later Insurtech Neobanks Remittance services	Ride Hailing (Uber) Driver Passenger Car Rental E-Scooter Bike Sharing Mobility Services Car Subscription Electronic Toll Parking Systems Electric Vehicle Charging Fleet Management	Online Casino Sport betting Online Lotteries Skill Gaming Virtual Goods In-Game Purchase Gaming with real money	Flights Hotels Loyalty Ocean Cruises Visa Immigration Travel agencies

Human Resources	Real estate	Healthcare	Education
Employment background checks Payroll services Benefits administration Remote work Relocation services Training Certification Loan Programs Freelancer Corporate Travel Corporate Expenses Time attendance	Property Purchase and Sale Rental Mortgage Property management	Patient registration Telemedicine Medical insurance claims Pharmacy Services	Student Enrollment Online Learning Scholarship Financial Aid Alumni

E-Commerce	Charity, non-profit	Supply Chain	Art
Marketplaces Payment Gateways Subscription Services	Donor verification Beneficiary verification Volunteer screening	Vendor verification Shipment tracking Custom Clearance	Auction participation Art dealers and galleries Art storage and transportation

Social media	Professional Services	Utilities	State
User account verification Influencer verification Marketplace Listings	Consulting services Accounting and tax services Recruitment agencies	Utility account registration electricity, water, gas Bill payment services	Vote Welfare Public Health Taxation Immigration Law enforcement Public records Education Employment Licensing

2.4 Main Legal Sources

The legal framework for KYC is defined by various international and national regulations:

Table 4: Legal Sources for KYC check per module

KYC Check	EU (European Union)	Switzerland	USA (United States)	Japan	Singapore
Identity Verification	4th AMLD (2015/849/EU)	GwG (Art. 3)	Bank Secrecy Act (31 U.S.C. §§ 5311-5330)	Act on Prevention of Transfer of Criminal Proceeds	MAS Notice 626
Person Verification Face	GDPR (Regulation (EU) 2016/679)	DPA (Art. 4)	FACTA (Fair and Accurate Credit Transactions Act)	Act on the Protection of Personal Information	PDPA (Personal Data Protection Act)
Person Detection Liveness	5th AMLD (2018/843/EU)	GwG (Art. 7)	CDD Rule (31 CFR 1010.230)	Act on Prevention of Transfer of Criminal Proceeds	MAS Notice 626
Security Features	5th AMLD (2018/843/EU)	GwG (Art. 3 and Art. 4)	Bank Secrecy Act (31 U.S.C. §§ 5311-5330)	Act on Prevention of Transfer of Criminal Proceeds	MAS Notice 626
Manual Review	4th AMLD (2015/849/EU)	GwG (Art. 6)	USA PATRIOT Act (Pub. L. 107-56)	Act on Prevention of Transfer of Criminal Proceeds	MAS Notice 626
Video in Person Ident	eIDAS Regulation (EU) No 910/2014	e-ID Regulation	FinCEN Guidance (FIN-2010-G001)	Act on Prevention of Transfer of Criminal Proceeds	MAS Notice 626
Address Verification	4th AMLD (2015/849/EU)	GwG (Art. 3 and Art. 5)	Bank Secrecy Act (31 U.S.C. §§ 5311-5330)	Act on Prevention of Transfer of Criminal Proceeds	MAS Notice 626

Sanction lists, PEP, crime	5th AMLD (2018/843/EU)	GwG (Art. 12 and Art. 15)	OFAC (Office of Foreign Assets Control)	Act on Prevention of Transfer of Criminal Proceeds	MAS Notice 626
Wallet and transaction check	5th AMLD (2018/843/EU)	GwG (Art. 10)	FinCEN Guidance (FIN-2019-G001)	Act on Prevention of Transfer of Criminal Proceeds	MAS Notice 626
Enhanced due diligence	5th AMLD (2018/843/EU)	GwG (Art. 9 and Art. 15)	USA PATRIOT Act (Pub. L. 107-56)	Act on Prevention of Transfer of Criminal Proceeds	MAS Notice 626

Abbreviations Table 4
AMLD: Anti-Money Laundering Directive
GwG: Geldwäschereigesetz (Anti-Money Laundering Act in Switzerland)
DPA: Data Protection Act (Switzerland)
BSA: Bank Secrecy Act (USA)
FACTA: Fair and Accurate Credit Transactions Act (USA)
CDD Rule: Customer Due Diligence Rule (USA)
OFAC: Office of Foreign Assets Control (USA)
MAS: Monetary Authority of Singapore
PDPA: Personal Data Protection Act (Singapore)
eIDAS: Electronic Identification, Authentication, and Trust Services (EU)

3. Milestone 2 with ID Verification, Liveness Check, Proof of Address, AML, Media Check and Enhanced Due Diligence

Milestone 2 includes:
a. ID-Verification Level 3 with Identity Verification, Proof of Address, Person verification face, Person detection liveness, Security Features,
b. AML with check sanction lists, PEP, crime,
c. media check and enhanced due diligence.

3.1 Levels of KYC

- KYC processes can be divided into several modular levels, building upon each other, offering an increasing degree of check.
- AML and KYT can be applied as an optional module with KYC Levels 1-2b and are applied starting level 3.
- EDD can be applied as an optional module with all KYC Levels and is applied in matches resulting from AML and KYT and is applied with an amount per transaction and linked transaction of 10.000 EUR (EU), 10.000 USD (USA), 15.000 CHF (Switzerland), 2.000.000 PY (Japan), 20.000 SGD (Singapore), 120.000 HDK (Hong Kong), 50.00 CNY (China), 1.000.000 INR (India).

Table 3: Levels of KYC and elements

Level/ module	Element	
1	Identity Verification	Basic identity verification involves collecting and validating minimal personal information such as name, address verification, date of birth, and government-issued ID.
2a	Person verification face	Moderate verification with enhanced document checks and address verification. Applied in medium-risk scenarios.
2b	Person detection liveness	Advanced verification, including biometric checks and more thorough document and background verifications. Used for higher-risk transactions.
3	Security Features	High-assurance verification, involving extensive checks, AML screening, and continuous monitoring. Necessary for high-value transactions and high-risk customers.
4	Manual review	Manual review involves a detailed examination of verification processes by trained personnel. This step is used to resolve discrepancies or confirm the accuracy of automated checks. It is particularly important in cases where automated systems flag potential issues or inconsistencies.
5	Video in person Live-Ident	Video in-person identification requires the individual to verify their identity through a live video call with a verification agent. This process ensures the highest level of assurance by allowing the agent to confirm the person's identity in real-time and verify the authenticity of their documents.
Address	Address verification	Address verification by document (utility bills, bank statements, government-issued documents, lease or rental agreements), electronic verification (address database, postal verification), direct (home visit, geolocation data).

AML	Sanction lists, PEP, crime	Sanction lists, PEP (Politically Exposed Persons), and crime checks involve screening individuals against global sanctions lists, watchlists for politically exposed persons, and databases of known criminals. This process helps identify high-risk individuals and prevent money laundering, terrorism financing, and other illicit activities.
EDD	Enhanced due diligence	Enhanced due diligence for very high-risk clients or transactions, including media checks, involving the most comprehensive checks and ongoing monitoring.
KYT	Wallet and transaction check	Wallet and transaction check entails monitoring cryptocurrency wallets and transactions for suspicious activities. This includes analyzing transaction patterns, checking against known risk factors, and ensuring compliance with AML regulations. It is crucial for preventing fraud and illicit transactions in the crypto space.
NFC	NFC readout	Enhance data readout quality and establish document authenticity.
eID	eID	Electronic identification via electronic identification card (eIC), which can be used for online and offline personal identification or authentication. The eIC, similar to a standard bank card, has printed identity information like personal details and a photograph, and an embedded RFID microchip. This chip stores the printed data, multiple photos for facial recognition, and potentially the holder's fingerprints. The card supports online authentication for services like age verification and e-government applications, and it can also store an electronic signature from a private company.

3.2 Provision of services in KYC environment requires approval from financial market authorities and certain certificates

The provision of those KYC services, including Identity Verification, Liveness Check, Proof of Address, AML, Media Check, and Enhanced Due Diligence, requires approval from relevant financial market authorities and adherence to stringent data protection regulations. Below are the details for various jurisdictions:

3.2.1. Licenses from Financial Market Supervisory Authority for KYC checks per jurisdiction

1. European Union (EU)
Financial Market Authority: Providers must obtain approval from relevant national financial market authorities within the EU member states. For example: France: Autorité des Marchés Financiers (AMF), Italy: Commissione Nazionale per le Società e la Borsa (CONSOB). Certificate: Must comply with EU-wide regulations such as the Fourth and Fifth Anti-Money Laundering Directives (4AMLD and 5AMLD).

2. Switzerland
Financial Market Authority: Swiss Financial Market Supervisory Authority (FINMA)
Certificate: Approval to provide services to financial institutions, including compliance with the Swiss Anti-Money Laundering Act (AMLA).

3. Germany
Financial Market Authority: Federal Financial Supervisory Authority (BaFin)
Certificate: Approval for offering services to financial institutions, ensuring compliance with the German Anti-Money Laundering Act (GwG).

4. United States (USA)
Financial Market Authority: Financial services providers must register with federal and state authorities, such as:
Federal: Financial Crimes Enforcement Network (FinCEN)
State: Various state financial regulators. Certificate: Compliance with the Bank Secrecy Act (BSA) and USA PATRIOT Act.

5. Japan
Financial Market Authority: Financial Services Agency (FSA)
Certificate: Approval for providing services, adhering to the Act on Prevention of Transfer of Criminal Proceeds.

6. China:
Financial Market Authority: People's Bank of China (PBoC).
Certificate: Approval for offering services, complying with the Anti-Money Laundering Law of the People's Republic of China.

3.2.2 Data protection authority registration per jurisdiction

1. European Union (EU):
Data Protection Law: General Data Protection Regulation (GDPR).
Registration: Providers must register with relevant national data protection authorities within the EU member states. Examples: France: Commission Nationale de l'Informatique et des Libertés (CNIL); Italy: Garante per la Protezione dei Dati Personali:

2. Switzerland:
Data Protection Law: Federal Act on Data Protection (FADP).
Registration: Providers must comply with FADP and may need to register with the Federal Data Protection and Information Commissioner (FDPIC).

3. Germany:
Data Protection Law: GDPR and the Federal Data Protection Act (BDSG)
Registration: Providers must comply with GDPR and BDSG, registering with relevant state data protection authorities.

4. United States (USA):
Data Protection Law: Varies by state; no federal-level comprehensive data protection law.
Examples: California: California Consumer Privacy Act (CCPA); New York: New York SHIELD Act.

5. Japan:
Data Protection Law: Act on the Protection of Personal Information (APPI)

Registration: Providers must comply with APPI and may need to register with the Personal Information Protection Commission (PPC).

6. China:
Data Protection Law: Personal Information Protection Law (PIPL)
Registration: Providers must comply with PIPL and may need to register with relevant regulatory authorities.

3.2.3 Certificates needed for KYC per jurisdiction

a. ISO/IEC 27001
An international standard for information security management systems. Companies providing identity verification services should be ISO/IEC 27001 certified to demonstrate their commitment to information security. Needed In: Global (including EU, Switzerland, Germany, USA, Japan, China, Singapore, other relevant jurisdictions)

b. ISO/IEC 27701
An extension to ISO/IEC 27001 for privacy information management, ensuring compliance with GDPR and other privacy regulations. Needed In: EU, Switzerland, Germany, USA, Japan, China, Singapore.

c. eIDAS Certification:
Certification under the EU Regulation on electronic identification and trust services for electronic transactions (eIDAS) for providing electronic identification services. Needed In: European Union (EU).

d. SOC 2 Type II:
Service Organization Control 2 Type II certification, which focuses on controls relevant to security, availability, processing integrity, confidentiality, and privacy. Needed In: Global (including EU, Switzerland, Germany, USA, Japan, China, Singapore, other relevant jurisdictions)

e. NIS2 Directive
Companies that provide identity verification services to sectors defined as critical infrastructure (e.g., financial services, healthcare, transport) in the EU will need to comply with NIS2. This includes implementing stringent cybersecurity measures and reporting incidents. Providers must ensure they have robust cybersecurity frameworks in place and conduct regular risk assessments and audits. Needed In: European Union (EU).

f. KRITIS (Critical Infrastructure):
In Germany, critical infrastructure (KRITIS) regulations apply to sectors such as energy, water, food, IT, telecommunications, health, transport, and finance. Companies providing services to critical infrastructure sectors must comply with the German IT Security Act (IT-Sicherheitsgesetz), which mandates the implementation of security measures and incident reporting. Providers must demonstrate they can protect critical systems and data from cyber threats, often requiring certifications like ISO/IEC 27001 and compliance with the Federal Office for Information Security (BSI) standards. Needed In: Germany.

3.3 Partners for this proposal for regulated, modular, certified KYC services

Companies such as Intrum, IDnow and others provide high-assurance identity verification services and hold the above-mentioned approvals to offer this service in 180+ countries and multiple languages. IAMX uses the services of Intrum and IDnow for this proposal.

3.4 API Documentation and SDK Documentation & Download for KYC verification per partner, per element

Table 4: API Documentation and SDK Documentation & Download

Level/ module	Element	Performed by	API, SDK
1	Identity Verification	Intrum, IDnow	https://www.idnow.io/developers/
2a	Person verification face		
2b	Person detection liveness		
3	Security Features		
Address	Address verification		
EDD	Enhanced due diligence		
AML	Sanction lists, PEP, crime	Intrum	Not public

3.5 What happens in ID-Verification Level 3 with Identity Verification, Proof of Address, Person verification face, Person detection liveness, Security Features?

ID-Verification Level 3 is a high-assurance process combining document and biometric checks. It involves collecting and verifying government-issued IDs, confirming addresses via recent utility bills or bank statements, and using advanced facial recognition for person verification. Liveness detection ensures the individual is present during verification, and security features on documents are examined for authenticity, preventing fraud and ensuring compliance, as described in 2.1 and in tables 3 and 4.

The identity verification services are performed through a standardized RESTful API using HTTP requests and JSON responses. This documentation outlines the API endpoints and how to implement these services within the IT infrastructure [https://www.idnow.io/developers/., offering a Postman Collection of API requests for easy access and debugging.

It is processed via the partners Intrum, IDnow and executed via auto-ident, an automated identity verification including the above-mentioned elements for personal identification. auto-ident automatically determines the type and version of the document (e.g., passport, ID card, driver’s license), retrieves data from the document, performs biometric comparison and liveness detection and verifies document authenticity. The process is supported via mobile apps for iOS and Android, SDKs for integration into customer-specific apps., web browser solution for integration via iFrame or as a standalone product.

3.5.1 KYC Outcomes and Compliance Obligations

Know Your Customer (KYC) is a crucial process used by financial institutions and other regulated companies to verify the identity of their clients. The primary purpose of KYC is to prevent identity theft, money laundering, terrorist financing, and financial fraud. The table outlines the possible outcomes of a KYC process and the obligations companies must adhere to.

The outcomes of a KYC check range from success, where the customer is approved after providing all necessary documentation and passing identity verification, to failure, where insufficient or fraudulent documentation leads to rejection. Other outcomes include pending status, where further information is needed; partial approval, which allows limited services; and deferred decisions due to external factors. Companies must ensure compliance with regulations by maintaining updated KYC records and documentation. They are obligated to report suspicious activities to authorities, typically through Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs). Customer notification is essential, providing transparency about the KYC process's outcome. Companies must keep detailed records securely stored and implement risk management strategies, regularly reviewing and updating processes to address high-risk customers. Regular audits and monitoring ensure compliance and effectiveness of the KYC process. Employee training on KYC procedures and the importance of compliance is vital. Additionally, protecting customer data against unauthorized access is a critical obligation to ensure privacy and security.

Table 5: Result options of a KYC Process and Obligations for the affected company

Category	Details
Result options of a KYC process	
Success/Approved	a. Customer has provided all necessary documents and information. b. Customer's identity and background successfully verified. c. Customer is deemed low risk and is approved for transactions or services.
Failure/Rejected	a. Insufficient documentation provided. b. Information provided does not match records or is fraudulent. c. Customer deemed high risk based on KYC checks.
Pending/Under Review	a. Additional information or documentation required. b. Inconsistencies or concerns need further investigation. c. Process temporarily paused awaiting further actions from customer or internal review.
Partial Approval	a. Customer approved for limited or restricted services. b. Additional verification may be required for full access.
Deferred	Decision postponed due to various reasons like insufficient data or external factors affecting verification process.

Obligations for the affected company	
Compliance with Regulations	a. Ensure KYC process complies with local and international regulations. b. Maintain updated records and documentation of all KYC processes and outcomes.
Reporting Obligations	a. Report suspicious activities or transactions to relevant authorities. b. File Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs) as required by law.
Customer Notification	a. Inform customer of the outcome of the KYC process. b. Provide reasons for rejection or additional requirements for pending cases.
Record Keeping	a. Maintain records of all KYC documentation and verification steps for a specified period (10 years). b. Ensure records are securely stored and easily retrievable for audits and inspections.
Risk Management	a. Regularly review and update risk assessment processes. b. Implement additional checks for high-risk customers or transactions.
Audit and Monitoring	a. Conduct regular audits of the KYC process to ensure compliance and effectiveness. b. Monitor ongoing customer activities to identify and mitigate risks.
Training and Awareness	a. Provide regular training to employees on KYC procedures and compliance requirements. b. Ensure staff are aware of the importance of KYC and the implications of non-compliance.
Data Protection	a. Ensure customer data is protected in compliance with data protection regulations. b. Implement measures to safeguard sensitive information from unauthorized access or breaches.

3.6 What happens in AML with check sanction lists, PEP, crime

In the context of Anti-Money Laundering (AML), the processes of checking sanction lists, Politically Exposed Persons (PEP), and monitoring for crime are critical components to ensure compliance with regulatory requirements and to prevent illegal activities such as money laundering and terrorism financing. Here's an overview of what happens with each aspect. All elements are performed via API AML to Intrum, as stated in table 4.

3.6.1. Sanction List Checks

Purpose
Sanction list checks are conducted to ensure that financial institutions do not engage in transactions with individuals, entities, or countries that are subject to sanctions imposed by governments or international bodies.

Process
- Screening: Financial institutions regularly screen their customer databases and transactions against updated sanction lists provided by regulatory authorities (e.g., OFAC, UN, EU).
- Match Handling: When a potential match is found, the institution must investigate further to determine if it is a true match or a false positive or do a mapping on accept / reject based on match handling.
- Action: If a true match is confirmed, the institution must take appropriate action, which can include freezing accounts, blocking transactions, and reporting to relevant authorities.

Table 6: Relevant sanction lists per jurisdiction

No	Sanctions List Name	Jurisdiction
1	United Nations Security Council (UNSC) Consolidated List	World
2	Office of Foreign Assets Control (OFAC) SDN List	USA
3	OFAC Consolidated Sanctions List	USA
4	European Union (EU) Consolidated List	EU
5	UK Treasury Sanctions List	UK
6	Canadian Sanctions List (Global Affairs Canada)	Canada
7	Australian DFAT Sanctions List	Australia
8	Swiss SECO Sanctions List	Switzerland
9	Japan MOF Sanctions List	Japan
10	Hong Kong Monetary Authority (HKMA) Sanctions List	Hong Kong
11	Monetary Authority of Singapore (MAS) Sanctions List	Singapore
12	UAE Central Bank Sanctions List	UAE
13	South African Reserve Bank (SARB) Sanctions List	South Africa
14	Reserve Bank of India (RBI) Sanctions List	India
15	New Zealand MFAT Sanctions List	New Zealand
16	FINTRAC Sanctions List	Canada
17	China MOFCOM Sanctions List	China

18	Russian Rosfinmonitoring Sanctions List	Russia
19	Brazilian Central Bank Sanctions List	Brazil
20	Mexican Treasury (SHCP) Sanctions List	Mexico
21	South Korean Ministry of Strategy and Finance Sanctions List	South Korea
22	Argentinian Financial Information Unit (UIF) Sanctions List	Argentina
23	Saudi Arabian Monetary Authority (SAMA) Sanctions List	Saudi Arabia
24	Indonesian Financial Services Authority (OJK) Sanctions List	Indonesia
25	Malaysian Central Bank (Bank Negara) Sanctions List	Malaysia
26	Qatar Central Bank Sanctions List	Qatar
27	Turkish Treasury and Finance Ministry Sanctions List	Turkey
28	Egyptian Central Bank Sanctions List	Egypt
29	Vietnam State Bank Sanctions List	Vietnam
30	Thai Ministry of Foreign Affairs Sanctions List	Thailand
31	Israeli Ministry of Finance Sanctions List	Israel
32	Pakistani State Bank Sanctions List	Pakistan
33	Colombian Financial Superintendence (SFC) Sanctions List	Colombia
34	Peruvian Financial Intelligence Unit (FIU) Sanctions List	Peru
35	Chilean Financial Market Commission (CMF) Sanctions List	Chile
36	Philippine Central Bank (BSP) Sanctions List	Philippines
37	Norwegian Ministry of Foreign Affairs Sanctions List	Norway
38	Icelandic Ministry for Foreign Affairs Sanctions List	Iceland
39	Swiss FINMA Sanctions List	Switzerland
40	Finnish Ministry for Foreign Affairs Sanctions List	Finland
41	Swedish Financial Supervisory Authority (FI) Sanctions List	Sweden
42	Danish Financial Supervisory Authority (FSA) Sanctions List	Denmark
43	Dutch Ministry of Finance Sanctions List	Netherlands
44	Belgian Financial Services and Markets Authority (FSMA) Sanctions List	Belgium
45	Austrian Financial Market Authority (FMA) Sanctions List	Austria
46	Irish Department of Foreign Affairs Sanctions List	Ireland
47	Portuguese Securities Market Commission (CMVM) Sanctions List	Portugal
48	Greek Ministry of Finance Sanctions List	Greece
49	Czech National Bank Sanctions List	Czech Republic
50	Polish Ministry of Finance Sanctions List	Poland

3.6.2. Politically exposed person (PEP) Checks

Purpose
Identifying and monitoring PEPs is crucial because these individuals hold positions of influence and may be at higher risk of being involved in bribery, corruption, or other illicit activities.

Process
- Identification: Financial institutions use PEP databases and other sources to identify customers or beneficial owners who are PEPs.
- Risk Assessment: PEPs are subject to enhanced due diligence (EDD), which involves a more thorough investigation of their financial activities and source of wealth.
- Ongoing Monitoring: PEPs are monitored continuously for any changes in their status or suspicious activities. This involves regular updates and re-assessment of their risk profiles.
- Option: Do a mapping on accept / reject based on match handling.

Table 7: PEP Categories

No	PEP Category	Description
1	Heads of State or Government	Current and former presidents, prime ministers, and monarchs.
2	Senior Politicians	Current and former senior officials in national, regional, or local government.
3	Senior Government Officials	High-ranking officials in executive, legislative, judicial, military, and administrative positions.
4	Members of Parliament or Similar Legislative Bodies	Current and former members of national parliaments, assemblies, and similar legislative bodies.
5	Senior Judicial Officials	Current and former judges, magistrates, and senior officials in the judiciary.
6	Senior Military Officials	High-ranking officers in the armed forces.
7	Senior Executives of State-Owned Corporations	Top executives in government-owned or controlled corporations.
8	Important Political Party Officials	Key members of major political parties.
9	Senior Diplomats	High-ranking diplomats, ambassadors, and senior officials in foreign services.
10	Members of Ruling Royal Families	Individuals holding significant positions within reigning royal families.
11	Heads of International Organizations	Current and former leaders of international organizations (e.g., UN, IMF, World Bank).
12	Board Members of Central Banks	Members of governing boards of central banks.
13	Regional and Local Government Leaders	Senior officials in regional or local government positions.
14	Senior Officials of Political Parties	Officials in significant roles within major political parties.
15	Senior Members of Religious Organizations	High-ranking officials in influential religious organizations.

16	Senior Officials of Non-Governmental Organizations (NGOs)	Leaders of prominent NGOs, particularly those involved in politics or large financial transactions.
17	Senior Executives of International Businesses	Executives in major multinational corporations.
18	Senior Executives in Media	Top officials in influential media organizations.
19	Family Members of PEPs	Immediate family members of PEPs, including spouses, children, and parents.
20	Close Associates of PEPs	Individuals known to have close business or personal relationships with PEPs.

3.6.3 Crime Monitoring

Purpose
Monitoring for criminal activities helps detect and prevent the misuse of financial systems for illegal purposes such as money laundering, fraud, and terrorist financing.

Process
- Transaction Monitoring: Financial institutions implement transaction monitoring systems that use rules and algorithms to flag suspicious transactions based on patterns, behaviors, and thresholds.
- Investigations: When a suspicious transaction is flagged, it is reviewed by compliance officers who analyze the details and context to determine if further investigation is required or do a mapping on accept / reject based on match handling for process automatization.
- Reporting: If a transaction is deemed suspicious, the institution must file a Suspicious Activity Report (SAR) with the appropriate regulatory body (e.g., FinCEN in the USA).

Table 8: Crime monitoring lists per jurisdiction

No	Source	List Name	Jurisdiction
1	Financial Action Task Force (FATF)	FATF High-Risk and Other Monitored Jurisdictions	World
2	Interpol	Interpol Most Wanted List	World
3	United Nations Office on Drugs and Crime (UNODC)	UNODC Drug and Crime Watch	World
4	Europol	Europol Most Wanted	EU
5	Office of Foreign Assets Control (OFAC)	OFAC Specially Designated Nationals (SDN) List	USA
6	Financial Crimes Enforcement Network (FinCEN)	FinCEN Suspicious Activity Reports (SARs)	USA
7	European Union (EU)	EU Financial Sanctions List	EU
8	UK National Crime Agency (NCA)	NCA Most Wanted List	UK

9	Australian Transaction Reports and Analysis Centre (AUSTRAC)	AUSTRAC Criminal List	Australia
10	Canadian Financial Transactions and Reports Analysis Centre (FINTRAC)	FINTRAC Criminal List	Canada
11	Swiss Financial Market Supervisory Authority (FINMA)	FINMA Criminal Watchlist	Switzerland
12	Monetary Authority of Singapore (MAS)	MAS Financial Crime Alerts	Singapore
13	Hong Kong Monetary Authority (HKMA)	HKMA Financial Crime List	Hong Kong
14	Financial Intelligence Unit (FIU) - India	FIU India Suspicious Transactions	India
15	Japan Financial Intelligence Center (JAFIC)	JAFIC Financial Crime List	Japan
16	Central Bank of the UAE	UAE Financial Crime Watch	UAE
17	Saudi Arabian Monetary Authority (SAMA)	SAMA Financial Crime List	Saudi Arabia
18	South African Reserve Bank (SARB)	SARB Financial Crime Watch	South Africa
19	Russian Federal Financial Monitoring Service	Rosfinmonitoring Watchlist	Russia
20	Brazilian Financial Intelligence Unit (COAF)	COAF Criminal List	Brazil
21	Mexican Financial Intelligence Unit	Mexico FIU Criminal List	Mexico
22	Financial Supervisory Service (FSS) - South Korea	FSS Korea Financial Crime List	South Korea
23	Argentine Financial Information Unit (UIF)	UIF Argentina Crime List	Argentina
24	Indonesian Financial Transaction Reports and Analysis Centre (PPATK)	PPATK Crime Watch	Indonesia
25	Turkish Financial Crimes Investigation Board (MASAK)	MASAK Crime Watchlist	Turkey

26	Central Bank of Malaysia (BNM)	BNM Financial Crime List	Malaysia
27	Central Bank of the Philippines (BSP)	BSP Crime Watch	Philippines
28	Financial Market Commission (CMF) - Chile	CMF Chile Crime List	Chile
29	State Financial Monitoring Service of Ukraine	SFMS Ukraine Financial Crime List	Ukraine
30	Central Bank of Nigeria (CBN)	CBN Financial Crime Watch	Nigeria

3.6.4 Obligations and procedures for AML in case of a match in the categories sanctions, pep, crime

Compliance Staff
The review and check of Anti-Money Laundering (AML) compliance are conducted by trained compliance staff. These professionals are skilled in identifying and verifying potential matches against sanctions, Politically Exposed Persons (PEPs), and crime lists. They use advanced tools, perform Enhanced Due Diligence (EDD), and cross-reference multiple databases to ensure accuracy. By maintaining up-to-date knowledge of regulatory requirements and employing rigorous verification processes, compliance staff play a crucial role in preventing financial crimes and ensuring the company adheres to legal and regulatory standards. Their expertise is vital in managing risks and maintaining the integrity of the financial system.

False positive match
Reviewing a potential false positive match in AML involves a detailed process to verify accuracy against sanctioned, PEP, or crime lists. This is the process: Begin with an initial assessment by comparing basic customer details (name, date of birth, nationality, address). Verify identifiers such as names, aliases, and government-issued IDs. Cross-reference with internal and third-party databases. Analyze transaction patterns and business activities. Conduct Enhanced Due Diligence (EDD) by interviewing the customer and requesting additional documentation. Utilize advanced tools like AI and biometric verification. Consult external AML compliance experts or regulatory bodies if needed. Document all findings and maintain a clear audit trail for future reference and regulatory inspections.

Ignore a match is not an option
Ignoring a false positive match in AML compliance is not permissible. The affected companies must thoroughly review all potential matches to comply with legal and regulatory requirements, avoiding non-compliance and associated penalties. Proper documentation and reporting of false positives are mandatory to maintain comprehensive records. Ignoring matches risks reputational damage and operational penalties. Best practices in compliance demand due diligence and maintaining a clear audit trail for transparency. Failure to address potential matches can result in substantial fines, legal action, and severe regulatory consequences. Thorough review processes ensure compliance and mitigate risks effectively.

Table 9: Obligations and response actions per match category

Step	Sanctions Matches	PEP Matches	Crime Matches
Initial Detection and Matching	Automated screening systems identify potential matches.		
Review and Verification	a. Review to determine if the match is a false positive. b. Conduct Enhanced Due Diligence (EDD) if match appears legitimate.		
Response Actions	a. Freeze accounts involved if match is confirmed. b. Report to relevant regulatory authorities within 24 hours, using the prescribed forms; U.S.: OFAC reporting form, EU: EU Sanctions Reporting Form, Germany: BAFA Sanctions Report Form, Switzerland: SECO Sanctions Report Form, Japan: METI Sanctions Report Form c. Ensure compliance with sanctions regulations.	a. Assess risk associated with doing business with a PEP. b. Implement enhanced monitoring. c. Internal reporting to senior management.	a. Detailed review of past and current transactions. b. File Suspicious Activity Report (SAR) within 30 days, using the prescribed forms: U.S.: FinCEN SAR Form, EU: FIU.net SAR Form, Germany: goAML SAR Form, Switzerland: MROS SAR Form, Japan: JAFIC SAR Form c. Coordinate with law enforcement and regulatory bodies.
Ongoing Monitoring and Controls	a. Regularly review and update customer profiles (at least annually). b. Train employees on AML policies (annually). c. Update screening systems with latest lists and requirements (ongoing).		
Documentation and Record-Keeping	a. Maintain detailed records of the match, review process, decisions made, and actions taken. b. Ensure actions are documented and auditable.		

3.7 What happens in media check and enhanced due diligence.

Media check and enhanced due diligence (EDD) are components of KYC risk management, particularly in compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.

Media Check
A media check involves searching for any adverse or negative information about an individual or entity in various media sources, including news articles, blogs, social media, and other publicly available information.

Process
1. Online Tool search based on keywords specific keywords related to the individual or entity being investigated, such as names, associated businesses, and relevant terms like "fraud," "money laundering," "scandal," etc.
2. Aggregate data.
3. Analysis: Reviewing and analyzing the collected information to identify any potential red flags or adverse media mentions; or do a mapping on accept / reject based on match handling for process automatization.

Purpose
Identify any past involvement in illegal activities, scandals, or unethical behavior.
Assess the reputational risk associated with the individual or entity.

3.8 Enhanced Due Diligence (EDD)
EDD is a thorough and comprehensive process of investigating and assessing higher-risk individuals or entities, going beyond the standard KYC due diligence procedures causing a ongoing AML-monitoring and proof of funds verification to ensure the legitimacy of the sources.

3.8.1 Incidents to activate EDD:

a. Specific Transaction Amounts:
- EU: 10,000 EUR per transaction or linked transactions.
- USA: 10,000 USD per transaction or linked transactions.
- Switzerland: 15,000 CHF per transaction or linked transactions.
- Japan: 2,000,000 JPY per transaction or linked transactions.
- Singapore: 20,000 SGD per transaction or linked transactions.
- Hong Kong: 120,000 HKD per transaction or linked transactions.
- China: 50,000 CNY per transaction or linked transactions.
- India: 1,000,000 INR per transaction or linked transactions.

Transactions meeting these thresholds typically require proof of funds verification to ensure the legitimacy of the sources.

b. AML Check Matches:
- Matches in Anti-Money Laundering (AML) checks related to sanctions, Politically Exposed Persons (PEP), and crime.
- Such matches trigger a media check and ongoing monitoring of the individual or entity.
- Within companies, an AML check is conducted on beneficial owners who are natural persons with a controlling stake.

- The threshold for a controlling stake typically ranges from a minimum of 10% to 25%, depending on the jurisdiction or regulatory requirements.

c. Unusual or Suspicious Activities:
- Unusual transaction patterns that deviate significantly from the normal activity of an account.
- Transactions that appear to be structured to avoid regulatory reporting requirements (e.g., smurfing).

d. Adverse Media Reports:
- Negative news or adverse media coverage about a client or beneficial owner indicating potential involvement in illegal activities or financial crimes.

e. Large Cash Transactions:
- Significant cash deposits or withdrawals, especially if they are inconsistent with the customer's known legitimate business or personal activities.

f. Non-face-to-face Business Relationships:
- Clients who establish business relationships without a face-to-face meeting, increasing the risk of identity fraud or misrepresentation.

g. Cross-Border Transactions:
- Significant or frequent cross-border transactions, particularly involving jurisdictions with weaker AML controls.

Purpose
Provide a deeper understanding of higher-risk customers and their potential risk to the organization.
Comply with regulatory requirements for AML and CTF.
Make informed decisions regarding the continuation, modification, or termination of a business relationship.

3.8.2 EDD on financial transactions Proof of Funds vs Proof of Origin of Funds
Enhanced Due Diligence (EDD) on financial transactions is a critical aspect of ensuring transparency and compliance within the financial sector. Two key components of EDD are Proof of Funds (PoF) and Proof of Origin of Funds (PoOF), each serving distinct but complementary purposes in the verification process. Proof of Funds involves providing evidence that verifies the availability of claimed funds, primarily to confirm that the money exists and is available for a specific transaction. This is typically used in high-value transactions, such as real estate purchases or large investments, and commonly involves documentation like bank statements or letters from financial institutions. On the other hand, Proof of Origin of Funds focuses on ensuring that the funds are legally obtained and aims to prevent financial crimes such as money laundering. This requires more comprehensive documentation, including pay stubs, tax returns, and business financial statements, to trace the source and history of the funds over time. PoOF is particularly crucial in high-risk transactions and scenarios involving high-risk clients. Together, PoF and PoOF play vital roles in confirming both the availability and the legality of funds, thereby enhancing the integrity and security of financial transactions.

Table 10: EDD on Proof of Funds / Source of Funds (SOF) vs Proof of Origin of Funds vs Source of Wealth (SOW)

Aspect	Proof of Funds / Source of Funds (SOF)	Proof of Origin of Funds	Source of Wealth (SOW)
Definition	Evidence verifying the availability of claimed funds and their immediate origin.	Documentation explaining the source and history of funds.	Verification of the origin and accumulation of an individual's or entity's total wealth.
Purpose	To confirm the money exists and is available for a specific transaction, ensuring it is legal.	To ensure funds are legally obtained and to prevent financial crimes.	To ensure that the overall wealth has been acquired legally and is consistent with the individual's or entity's financial profile.
Common Documentation	Bank statements, Letters from financial institutions, Recent investment account statements, Deposit receipts or certificates of deposit, Transfer receipts, Loan agreements	Pay stubs, employment contracts, Business financial statements, tax returns, Sale agreements, transfer deeds, Probate documents, wills, Gift letters, donor's bank statements, Dividends statements, capital gains reports	Comprehensive financial history including tax returns, business income statements, property deeds, investment portfolios, inheritance documents, etc.
When Used	High-value transactions, Verifying availability of funds, Ensuring funds for a specific transaction are legitimate	High-risk clients or transactions, Ensuring funds are not from illicit activities	Assessing high-net-worth individuals, private banking, wealth management, high-value transactions
Focus	Confirms the existence and availability of money, and the immediate origin and legality of the money being used in a transaction.	Establishes the legal origin and acquisition history of money.	The overall legitimacy of how wealth was accumulated over time.

Documentation Timeline	Typically current financial status.	Can include historical documents showing a trail over time.	Extensive historical financial documentation
Usage	Immediate transactions requiring proof of liquidity.	Assessing the legality and history of funds, particularly in high-risk scenarios.	Providing a comprehensive financial background, especially for high-value or high-risk scenarios
Example Scenarios	Real estate purchases, Large deposits or investments, Large purchases, real estate transactions	AML compliance checks, High-risk or unusual transactions, Cross-border transactions	Private banking, high-value investments, regulatory compliance for high-net-worth individuals
Triggering Incidents	Large purchases, Real estate transactions, Investment activities	Transactions with high-risk clients, Cross-border transactions, Unusual or suspicious transactions	Opening private banking accounts, High-value investments, Regulatory compliance for high-net-worth individuals, Inheritance or large windfalls
Outcome if Unsuccessful	Transaction cannot proceed, Increased scrutiny, Possible account closure	Transaction blocked, Report to authorities, Enhanced due diligence	Denial of services, Increased monitoring, Potential account closure
Obligations if Unsuccessful	Report suspicious activity to authorities, Enhanced monitoring of the customer, Compliance with regulatory requirements for suspicious transactions	Immediate reporting to Financial Intelligence Units (FIUs) or regulatory bodies, Implementation of enhanced due diligence measures, Restriction or suspension of account activities	Notify regulatory authorities, Conduct a comprehensive review of the customer's profile, Implement restrictive measures on account activities, Ensure compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) laws

Table 11: Event to cause EDD as Proof of Funds / Source of Funds (SOF) vs Proof of Origin of Funds vs Source of Wealth (SOW)

Event/Trigger	Proof of Funds (SOF)	Proof of Origin of Funds	Source of Wealth (SOW)
High-Value Transactions	Yes	No	Yes
Large Deposits or Investments	Yes	No	Yes
Real Estate Purchases	Yes	No	Yes
AML Compliance Checks	No	Yes	No
High-Risk Clients or Transactions	No	Yes	Yes
Cross-Border Transactions	No	Yes	No
Transactions Involving High-Risk Jurisdictions	No	Yes	Yes
Complex Ownership Structures	No	Yes	Yes
Adverse Media Reports	No	Yes	Yes
Politically Exposed Persons (PEP) Status	No	Yes	Yes
Non-face-to-face Business Relationships	No	Yes	No
Unusual or Suspicious Transaction Patterns	No	Yes	Yes
Transactions Involving Cryptocurrencies	No	Yes	No
Sale of Assets	No	Yes	Yes
Inheritance	No	Yes	Yes
Gifts min 10,000 EUR / USD	No	Yes	Yes