KNOW YOUR TRANSACTION POLICY

PayNox EOOD

ID number: 208071994

Legal address: Bulgaria, City of Burgas, 19 Marahydyk St., fl. 2, office 1

Table of contents

INTRODUCTION

The Know Your Transaction (KYT) Policy is a key of PayNox's Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) framework, designed to monitor and analyze transactions in real-time to detect suspicious activities. Unlike Know Your Customer (KYC), which focuses on verifying customer identity, KYT emphasizes understanding transactional behavior, identifying anomalies, and preventing illicit financial activities such as money laundering, fraud, and terrorist financing.

PayNox EOOD is committed to adhering to Bulgarian AML laws, the European Union's 6th Anti-Money Laundering Directive (6AMLD), and the recommendations set forth by the Financial Action Task Force (FATF). This policy integrates real-time transaction monitoring, enhanced due diligence (EDD), and regulatory reporting to comply with financial supervision requirements under Bulgaria's Financial Supervision Commission (FSC).

By implementing KYT, financial institutions and cryptocurrency exchanges can track the flow of funds, assess risks associated with transactions, and ensure compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations. Through a combination of automated monitoring systems and manual reviews, KYT helps organizations identify high-risk transactions, conduct thorough investigations, and take appropriate actions, such as freezing funds or reporting suspicious activities to regulatory authorities.

This policy ensures that all transactions align with regulatory requirements and internal risk management frameworks, helping to safeguard the integrity of financial systems while enhancing trust and security for customers and stakeholders.

DEFINITION

Definitions

Know Your Transaction (KYT): A compliance process that focuses on monitoring and analyzing financial transactions in real-time to detect suspicious activities, prevent financial crimes, and ensure regulatory compliance.

Suspicious Transaction: Any transaction that appears unusual, inconsistent with a customer's typical behavior, or indicative of potential money laundering, fraud, or terrorist financing.

Transaction Monitoring System: An automated tool used by financial institutions and cryptocurrency exchanges to track, analyze, and flag potentially suspicious transactions based on predefined risk parameters.

Enhanced Due Diligence (EDD): A deeper level of investigation applied to high-risk transactions or customers, requiring additional verification and documentation to assess the legitimacy of funds.

Politically Exposed Person (PEP): An individual who holds or has held a high-profile public position and may pose a higher risk for involvement in financial crimes due to their influence and access to resources.

Sanctions Screening: The process of checking transactions and involved parties against global sanctions lists to prevent dealings with restricted or blacklisted entities.

Red Flags: Indicators of potentially suspicious activities, such as rapid movement of large sums, transactions involving high-risk jurisdictions, or frequent small deposits structured to avoid detection.

Risk-Based Approach (RBA): A methodology that assesses and prioritizes financial risks, applying stricter monitoring and controls to high-risk transactions while maintaining efficiency for lower-risk activities.

Suspicious Activity Report (SAR): A formal report submitted to regulatory authorities when a transaction is suspected to be linked to illegal activities, such as money laundering or fraud.

Blockchain Analytics: Tools used in cryptocurrency transactions to trace the origin and movement of digital assets, helping to identify illicit activities such as mixing, tumbling, or transactions with sanctioned wallets.

These definitions form the foundation of an effective KYT policy, ensuring clarity and consistency in monitoring, assessing, and reporting financial transactions.

SCOPE

The KYT Policy applies to all financial transactions processed by PayNox, including deposits, withdrawals, fund transfers, and cryptocurrency trades. It ensures compliance with Bulgarian AML laws, EU AMLD regulations, FATF recommendations, and GDPR data protection standards. It covers the monitoring, assessment, and reporting of transactional activities to detect and prevent financial crimes such as money laundering, fraud, terrorist financing, and sanctions violations.

This policy is applicable to all customers, counterparties, and third parties engaging in financial transactions with the institution. It extends to both individual and corporate accounts, ensuring that all transactional activities align with regulatory requirements and internal risk management frameworks.

The KYT policy applies across various transaction types, including deposits, withdrawals, fund transfers, cryptocurrency trades, and payments. It is implemented through automated monitoring systems, manual reviews, and enhanced due diligence

(EDD) where necessary. High-risk transactions involving politically exposed persons (PEPs), high-risk jurisdictions, or potential structuring (smurfing) will undergo enhanced due diligence (EDD) and real-time analysis using blockchain analytics tools (e.g., Chainalysis, TRM Labs, Elliptic) are subject to heightened scrutiny.

Additionally, the policy ensures compliance with global AML/CTF regulations, requiring continuous adaptation to emerging financial crime threats, regulatory updates, and advancements in transaction monitoring technologies.

CORE PRINCIPLES

The Know Your Transaction (KYT) Policy is built on key principles that ensure the effective monitoring, detection, and prevention of financial crime.

Risk-Based Approach (RBA) – Transactions are monitored based on their risk level, with high-risk activities receiving enhanced scrutiny, while low-risk transactions follow streamlined procedures.

Real-Time Monitoring – All transactions are assessed in real time using automated systems to detect suspicious activities, unusual patterns, and compliance violations.

Enhanced Due Diligence (EDD) – High-risk transactions, such as those involving politically exposed persons (PEPs) or high-risk jurisdictions, undergo deeper investigation, requiring additional documentation and verification.

Suspicious Transaction Reporting – Any flagged transactions that meet regulatory thresholds for suspicion are escalated for further review, with Suspicious Activity Reports (SARs) filed with relevant authorities if necessary.

Sanctions and Compliance Screening – Transactions are screened against sanctions lists, watchlists, and blacklisted entities to prevent dealings with restricted or high-risk parties.

Transparency and Traceability – In cryptocurrency transactions, blockchain analytics tools are used to track the origin and movement of digital assets, ensuring funds are not linked to illicit activities like mixing, tumbling, or darknet transactions.

Continuous Improvement – The KYT framework is regularly updated to adapt to evolving regulatory requirements, emerging financial crime threats, and advancements in transaction monitoring technologies.

By applying these principles, the KYT policy strengthens financial security, regulatory compliance, and risk management, protecting the institution from illicit financial activities.

RISK-BASED APPROACH

The Know Your Transaction (KYT) Policy follows a Risk-Based Approach (RBA) to ensure that financial transactions are monitored and assessed according to their risk level. This method allows financial institutions and cryptocurrency exchanges to allocate resources efficiently, applying stricter controls to high-risk transactions while minimizing unnecessary disruptions to legitimate activities.

Under the Risk-Based Approach (RBA), transactions are classified into low, medium, and high-risk categories based on:

- Transaction Size (e.g., exceeding EUR 10,000 triggers automatic review)
- Geographic Risk (transactions involving sanctioned or high-risk jurisdictions)
- Customer Risk Profile (PEPs, businesses in high-risk sectors such as gambling or remittance services)
- Transaction Behavior (rapid movements, frequent large deposits without clear justification)

We analyze transaction behaviors in real time, detecting anomalies based on predefined risk parameters. When a transaction triggers a red flag, compliance analysts conduct a manual review, verifying supporting documentation and customer justifications. All flagged transactions undergo further scrutiny, and in suspicious cases, PayNox will submit a Suspicious Activity Report (SAR) to the Bulgarian Financial Intelligence Directorate.

The risk-based approach ensures that legitimate transactions are processed efficiently while preventing illicit financial activities, balancing security, compliance, and customer experience. Institutions regularly update their risk models to adapt to evolving threats, regulatory changes, and emerging financial crime techniques, ensuring continuous improvement in transaction monitoring.

REAL-TIME MONITORING

Real-time monitoring is a critical component of the Know Your Transaction (KYT) Policy, enabling financial institutions and cryptocurrency exchanges to detect and respond to suspicious transactions as they occur. Unlike traditional batch processing, real-time monitoring ensures that every transaction is analyzed instantaneously, reducing the risk of financial crime, fraud, money laundering, and sanctions violations.

Using automated transaction monitoring systems, transactions are screened against predefined risk parameters such as amount, frequency, geographic location, counterparties, and behavioral patterns. If a transaction appears unusual—such as a sudden large transfer, frequent small deposits designed to evade detection, or

transactions involving high-risk jurisdictions are immediately flagged for further review.

When a transaction is flagged, compliance analysts conduct a manual assessment, verifying the customer's profile, transaction history, and supporting documentation. If necessary, the institution may request additional information from the customer or apply Enhanced Due Diligence (EDD). Suspicious transactions that meet regulatory thresholds are escalated for further investigation, and a Suspicious Activity Report (SAR) may be filed with regulatory authorities.

Real-time monitoring enhances compliance, security, and risk management by allowing financial institutions to proactively prevent illicit activities rather than react after the fact. As financial crime tactics evolve, transaction monitoring systems are continuously updated to adapt to new threats, ensuring ongoing regulatory compliance and the protection of financial assets.

MANUAL MONITORING SYSTEM

While automated systems play a crucial role in transaction monitoring, manual monitoring remains an essential layer of oversight within the Know Your Transaction (KYT) Policy. A manual monitoring system involves human review and analysis of flagged transactions, providing deeper insight into complex cases that automated systems might not fully assess.

When a transaction is flagged due to unusual patterns, high-risk jurisdictions, large amounts, or other risk indicators, compliance analysts manually investigate the activity. This includes reviewing transaction details, checking the customer's profile and transaction history, and analyzing supporting documents such as invoices, contracts, or proof of funds. If necessary, the compliance team may contact the customer for additional clarification.

Manual monitoring is especially useful for high-risk transactions, such as those involving politically exposed persons (PEPs), cryptocurrency transfers with obfuscation techniques (mixing or tumbling), or accounts with rapid and irregular movements of funds. Unlike automated systems, which rely on predefined rules, manual monitoring allows compliance officers to apply judgment, context, and real-world experience to determine whether a transaction is suspicious.

If a transaction remains questionable after review, it is escalated to senior compliance officers, and a Suspicious Activity Report (SAR) ay be submitted to regulatory authorities. If the transaction is deemed legitimate, it is cleared, and the findings are documented for future audits and compliance tracking.

Manual monitoring complements automated transaction monitoring systems, ensuring that complex and nuanced cases receive appropriate scrutiny. This hybrid approach

strengthens risk management, regulatory compliance, and fraud prevention, balancing efficiency with human expertise.

LIST OF THRESHOLDS, RISK TOLERANCE AND RISK CATEGORIZATION FOR ILLICIT OPERATIONS

Thresholds, risk tolerance, and risk categorization are essential components of a Know Your Transaction (KYT) Policy, ensuring that financial institutions and cryptocurrency exchanges can effectively detect and mitigate illicit operations.

Transaction thresholds are predefined limits that trigger alerts when exceeded. High-value transactions, typically those above $10,000, are subject to additional verification and regulatory reporting. However, illicit actors often attempt to bypass these limits by structuring transactions just below the reporting threshold. Multiple small transactions, especially those just under compliance limits, can indicate smurfing or layering activities used for money laundering. Another key indicator of suspicious activity is rapid movement of funds, where transactions occur in quick succession across multiple accounts or jurisdictions. This behavior suggests an attempt to evade detection by dispersing funds quickly. Similarly, high-volume cryptocurrency transactions that involve privacy wallets or coin mixers raise concerns, as they are commonly used to obscure the origin of funds.

Risk tolerance determines how much exposure an institution is willing to accept before taking action. Low-risk tolerance applies to transactions with sanctioned entities, blacklisted wallet addresses, and darknet marketplaces, which result in immediate rejection and mandatory reporting. Transactions involving politically exposed persons (PEPs) or those originating from high-risk jurisdictions fall under medium tolerance, meaning they require enhanced due diligence (EDD) and additional documentation. Meanwhile, routine transactions within a verified customer's usual activity range pose minimal concern and fall within acceptable limits, though they are still subject to periodic review.

Risk categorization further refines the approach to transaction monitoring by classifying transactions and customers based on their risk level. Low-risk transactions involve verified individuals or businesses with consistent financial behavior that aligns with their profile. These transactions usually occur between regulated financial institutions or within an organization's ecosystem where compliance measures are already in place. Medium-risk activities, however, may involve customers from industries with higher AML concerns, such as gambling or remittance services. Occasional high-value transactions may also require additional scrutiny, particularly if they lack a clear economic purpose. The use of privacy-enhancing tools like CoinJoin or privacy coins in small amounts may not immediately indicate illicit intent but still necessitates closer monitoring.

At the highest risk level, transactions linked to sanctioned countries, darknet markets, or known illicit actors demand immediate escalation. Transactions that leverage mixing, tumbling services, or frequent chain-hopping between multiple cryptocurrencies are strong indicators of money laundering. Additionally, customers who suddenly change their transaction patterns, such as making large international transfers without prior history, warrant further investigation.

By defining clear thresholds, establishing risk tolerance levels, and applying risk categorization, financial institutions can systematically detect, investigate, and mitigate illicit financial activities while maintaining compliance with regulatory requirements. This structured approach ensures that legitimate transactions are processed smoothly, while suspicious activities are promptly flagged and addressed.

REVIEW OF ALERTS

The review of alerts is a crucial step in transaction monitoring, ensuring that flagged activities are properly assessed for potential financial crime risks. When an automated system detects unusual transactions, it generates alerts based on predefined risk rules, such as large or sudden transfers, transactions involving high-risk countries, or patterns indicative of structuring or money laundering.

Once an alert is triggered, compliance analysts conduct an initial assessment to determine its validity. They analyze transaction details, customer profiles, and historical activity to assess whether the alert is a false positive or requires further investigation. Transactions that match legitimate patterns or have clear justifications may be cleared, while those showing inconsistencies or suspicious elements are escalated for deeper review.

During the review, analysts may verify the customer's identity, check against sanctions lists, and examine supporting documents to validate the legitimacy of the transaction. If the alert is deemed high-risk, it is forwarded to senior compliance officers or legal teams for further scrutiny. In cases where suspicious activity is confirmed, a Suspicious Activity Report (SAR) may be filed with regulatory authorities, and additional actions, such as freezing funds or blocking transactions, may be taken.

Effective alert review processes involve continuous refinement of detection rules and feedback loops between manual reviewers and automated systems. By improving accuracy and reducing false positives, organizations can ensure compliance while efficiently identifying and mitigating financial crime risks.

SAMPLE OF HOW ALERTS ARE RESOLVED AND REPORTED INTERNALLY

Scenario: Unusual Large Transaction

A customer who typically conducts small transactions under $5,000 suddenly initiates a $100,000 transfer to an overseas account. The automated system flags this as unusual based on the customer’s historical activity and the destination being a high-risk jurisdiction.

The analyst receives the alert and reviews the customer's profile, past transactions, and risk rating.

The analyst checks whether there is a valid business justification for the transaction, such as recent changes in income, business expansion, or investment activity.

External databases, sanctions lists, and politically exposed persons (PEP) checks are conducted to verify if the recipient or sender is linked to any financial crime risks.

If no immediate red flags are found, the analyst may contact the customer for additional clarification and documentation.

The customer is asked to provide supporting documents, such as invoices, contracts, or bank statements, to justify the transfer.

If the explanation aligns with the customer’s profile and legitimate business activity, the transaction may be cleared.

If the response is insufficient, contradictory, or raises additional concerns, the alert is escalated for further investigation.

If the transaction remains suspicious after the initial review, the case is escalated to senior compliance officers.

Enhanced Due Diligence (EDD) is conducted, including a deeper background check on the customer and recipient.

Additional transaction monitoring is performed to assess whether this activity is part of a broader pattern of suspicious behavior.

If the transaction is legitimate: The case is documented, and the alert is marked as resolved. The customer’s risk profile may be updated if necessary.

If the transaction is suspicious: A Suspicious Activity Report (SAR) is prepared and submitted to regulatory authorities, detailing the transaction, risk factors, and investigative findings. The customer may be monitored more closely or subject to account restrictions.

The case is logged into the compliance system for future reference and regulatory audits.

Patterns from resolved alerts are analyzed to improve automated detection systems and reduce false positives.

Compliance teams conduct internal discussions to refine monitoring strategies based on emerging risks.

By following this structured process, organizations ensure regulatory compliance, mitigate financial crime risks, and maintain a strong risk management framework.

Scenario: Structured Cash Deposits

A customer deposits $9,800 in cash multiple times over a short period, just below the $10,000 reporting threshold for large cash transactions. The automated monitoring system detects a pattern of potential structuring, a common method used to evade anti-money laundering (AML) reporting requirements.

The compliance analyst reviews the customer's account history, noting that the individual typically deposits smaller amounts and has no prior pattern of large cash transactions.

The analyst checks whether the customer has a valid reason for making multiple deposits just below the reporting threshold.

External databases, sanctions lists, and politically exposed persons (PEP) checks are conducted to verify if the customer has any known connections to financial crime.

If the deposits appear legitimate, such as proceeds from a business or legal cash transactions, the alert may be resolved at this stage.

The compliance team reaches out to the customer for clarification on the source of funds.

The customer claims the deposits are personal savings but cannot provide supporting documents such as income statements, business records, or receipts.

The explanation raises concerns, as legitimate cash deposits are typically more transparent and supported by documentation.

The case is escalated to senior compliance officers due to concerns that the customer may be attempting to structure transactions to avoid reporting obligations.

Additional transaction monitoring is conducted to identify other related activities, such as withdrawals, transfers, or linked accounts showing similar behavior.

The compliance team assesses whether the customer has previous suspicious activity or if this pattern is isolated.

If the deposits are justified: The case is documented, the alert is marked as resolved, and the customer's risk profile is updated.

If the deposits remain suspicious: A Suspicious Activity Report (SAR) is filed with regulatory authorities detailing the transaction pattern, risk indicators, and investigation findings.

The customer may be placed under ongoing monitoring, and restrictions may be applied to the account if necessary.

The case is logged into the compliance system for audit and regulatory review.

The compliance team analyzes similar past cases to determine if system rules need adjustments to better detect structuring attempts.

Training sessions may be conducted for staff to improve awareness of structuring techniques and enhance detection measures.

By following this structured process, the organization ensures compliance with AML regulations, reduces financial crime risks, and strengthens its monitoring systems against evolving threats.

ENHANCED DUE DILIGENCE (EDD)

Enhanced Due Diligence (EDD) is a critical process embedded within the Know Your Transaction (KYT) policy, which ensures a heightened level of scrutiny for transactions that may pose a higher risk of financial crimes such as money laundering, terrorist financing, and fraud. While standard due diligence involves basic verification of customers and transactions, EDD is triggered when there are indications that the transaction or customer activity could be linked to illicit behavior or when the risks involved are more complex.

The purpose of EDD is to provide a deeper, more comprehensive investigation into high-risk transactions. This process is designed to safeguard financial institutions and cryptocurrency exchanges from inadvertently facilitating illegal activities. It allows them to remain compliant with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations by ensuring that all transactions meet the standards for transparency and legitimacy.

EDD is applied when transactions meet **high-risk criteria**, such as:

- Large transactions inconsistent with customer profile
- Transactions involving high-risk jurisdictions or businesses with opaque structures
- Use of privacy coins (e.g., Monero, Zcash) or mixing/tumbling services
- Unusual crypto-to-fiat or fiat-to-crypto conversions

The process of Enhanced Due Diligence is much more thorough than standard procedures. It begins with the collection of additional information about the customer and the transaction. This may include obtaining documents such as bank statements, business contracts, or records that justify the movement of funds. Institutions may also

rely on third-party verification sources, including government databases, international sanctions lists, and commercial tools that can validate whether the parties involved are linked to criminal organizations, sanctioned entities, or politically exposed individuals.

EDD procedures include:

- Verification of Source of Funds (SoF) & Source of Wealth (SoW)
- Additional identity checks
- Extended transaction history analysis
- Direct customer outreach for justification

If a transaction remains suspicious after EDD, PayNox will escalate the case to senior compliance officers and regulatory bodies.

Once the information has been gathered, transaction monitoring becomes more intensive. Analysts will examine the entire transaction history, look for patterns that deviate from the customer's usual behavior, and assess whether the current transaction fits the expected profile. If, for example, a customer who typically transfers funds to domestic accounts suddenly sends large sums to an overseas account in a high-risk region, it would trigger an in-depth investigation to understand the nature of the transaction and the potential risks involved.

In some cases, it may be necessary to contact the customer directly to clarify the reasons behind the flagged transaction. This communication may involve requesting supporting documents, such as proof of the source of funds, invoices, or even a detailed explanation of the business rationale behind the transaction. If a customer is transferring large amounts of money to a region known for high corruption or conflict, asking for a justification ensures that the transaction is not part of a money laundering scheme or other illicit activity.

However, EDD doesn't stop with the completion of a transaction. High-risk customers or flagged transactions are subject to ongoing monitoring to track any further suspicious activities. This continuous review ensures that financial institutions are not inadvertently allowing further illicit activities, especially in cases where initial scrutiny may not have revealed all potential risks.

Throughout the EDD process, detailed documentation is maintained, ensuring that all actions taken—such as the analysis, customer communication, and final decisions—are well recorded. This documentation is crucial not only for internal audit purposes but also for regulatory compliance. If the investigation leads to suspicions of illegal activities, the institution may need to file a Suspicious Activity Report (SAR) with the relevant authorities. This report details the concerns, the findings of the investigation,

and the reasoning for suspecting that the transaction may be connected to money laundering or other financial crimes.

SUSPICIOUS TRANSACTION REPORTING

Suspicious Transaction Reporting (STR) is a key part of the Know Your Transaction (KYT) policy, designed to help financial institutions identify and address potential illegal activities like money laundering, terrorist financing, or fraud. When conducting regular transaction monitoring, institutions may detect transactions that stand out as unusual or out of place compared to a customer's usual behavior or the transaction's stated purpose. These flags prompt a deeper investigation to determine if the transaction could be illicit.

A transaction becomes suspicious when it involves patterns or activities that seem inconsistent with normal business practices. For instance, a customer who usually makes small transactions may suddenly transfer large sums of money, or there may be transactions linked to high-risk countries known for corruption or poor financial regulation. Other indicators might include transactions that are excessively complex or lack a clear, legitimate business purpose, such as money being moved without explanation or justification. Furthermore, customer behavior, such as being evasive about transaction details or unwilling to provide necessary documents, can also be a red flag that warrants further scrutiny.

Once a suspicious transaction is flagged, the financial institution will launch a thorough investigation to determine its legitimacy. This often involves collecting additional information from the customer or reviewing historical transactions. The findings from this investigation are carefully documented to ensure transparency and to meet legal requirements. If the institution concludes that the transaction is suspicious, it must report it to the relevant authorities, often the Financial Intelligence Unit (FIU) or another regulatory body, in accordance with the jurisdiction's laws.

Filing a Suspicious Transaction Report (STR) is a legal obligation, and it must contain detailed information about the transaction, the individuals involved, and the reasons why the institution believes it may be linked to criminal activity. Institutions are generally prohibited from informing the customer that a report has been filed to avoid alerting those involved in the suspicious transaction and potentially interfering with an ongoing investigation.

The regulatory authorities receiving the STR will analyze the report and may initiate further investigations. In some cases, financial institutions might be instructed to take additional steps, such as freezing the transaction or placing a hold on the funds until the authorities have completed their review.

Overall, Suspicious Transaction Reporting is an essential safeguard that helps financial institutions prevent illegal activities and protect the financial system. By detecting and reporting suspicious transactions, institutions play a critical role in maintaining compliance with regulatory standards and contributing to the global effort to combat money laundering and other financial crimes.

SANCTIONS AND COMPLIANCE SCREENING

Sanctions and compliance screening is an essential process within financial institutions and cryptocurrency exchanges to ensure adherence to national and international laws aimed at preventing illegal activities like money laundering, terrorist financing, and fraud. This process involves checking transactions, customers, and business partners against sanctions lists, watchlists, and other databases to identify any entities or individuals subject to legal restrictions.

PayNox employs automated and manual screening to ensure transactions comply with international sanctions lists, including:

- United Nations (UN) Sanctions List
- European Union (EU) Financial Sanctions
- U.S. Office of Foreign Assets Control (OFAC)
- Interpol & Local Bulgarian Watchlists

Any transaction involving sanctioned entities or flagged counterparties is blocked immediately, and a SAR is filed with regulatory authorities.

The primary purpose of sanctions and compliance screening is to prevent financial institutions from inadvertently engaging in transactions with parties who are involved in illicit activities or are prohibited under international laws. Financial regulations often require institutions to screen transactions and parties to ensure that they are not dealing with individuals or entities that are subject to economic sanctions, such as those imposed by the United Nations, the European Union, or the U.S. Treasury's Office of Foreign Assets Control (OFAC). These sanctions could target individuals, organizations, or entire countries and are intended to limit their access to financial services to curb illegal activities like terrorism, drug trafficking, or human rights violations.

In the screening process, financial institutions review their customer databases, as well as transactions, against a variety of watchlists that include individuals or entities associated with criminal activity or those that are specifically prohibited from engaging in financial activities due to sanctions. This is often done through automated screening systems that cross-check all relevant transaction details—such as names, account

numbers, and countries of operation—against these sanction lists. If a match or "hit" occurs, the transaction or the individual is flagged for further investigation.

Compliance screening also involves ensuring that transactions comply with local and international anti-money laundering (AML) regulations and anti-terrorism financing (CTF) laws. This process may include assessing whether the transaction patterns align with legal and regulatory standards, monitoring for unusual or suspicious behavior, and verifying the legitimacy of customers and their funds. By integrating sanctions and compliance screening into their daily operations, institutions mitigate the risk of processing transactions that could lead to significant financial penalties or reputational damage.

In cases where a match is found during the screening process, the institution will initiate further steps, such as enhanced due diligence, to verify the legitimacy of the transaction. If the customer or transaction is confirmed to be linked to sanctions violations, the institution may be required to block the transaction, freeze accounts, and report the matter to the relevant authorities.

Ultimately, sanctions and compliance screening is a proactive measure that helps prevent financial institutions from becoming vehicles for criminal activities. It ensures that institutions remain compliant with national and international regulatory frameworks and uphold the integrity of the global financial system.

INTERNAL AUDITS & COMPLIANCE MONITORING

To ensure continuous improvement and adherence to Bulgarian AML laws and EU regulations, PayNox conducts:

- Quarterly internal audits of transaction monitoring processes
- Annual regulatory compliance assessments
- Ongoing training for compliance officers on emerging AML risks
- Real-time system updates to detect new laundering tactics

These audits provide insights into improving detection mechanisms and reducing false positives in transaction monitoring.

DATA RETENTION & PRIVACY COMPLIANCE

PayNox complies with GDPR and AML data retention laws by securely storing transaction records and customer due diligence (CDD) documents for a minimum of 5 years, as mandated by EU AMLD and Bulgarian financial regulations.

Customer data is only shared with regulatory authorities as required by law, ensuring full compliance with data protection and privacy standards.

CONTINUOUS IMPROVEMENT

Continuous improvement in Know Your Transaction (KYT) processes is essential for ensuring that financial institutions and other regulated entities are always prepared to identify, mitigate, and prevent risks related to money laundering, terrorist financing, and other illicit activities. Since the financial landscape and criminal tactics evolve rapidly, maintaining an effective KYT program requires ongoing efforts to enhance transaction monitoring systems, update procedures, and adapt to new regulatory changes. Continuous improvement in KYT involves a dynamic and proactive approach to adapt to these evolving challenges.

One critical element of continuous improvement in KYT is regularly evaluating the performance of the transaction monitoring systems. Financial institutions rely on automated systems to flag suspicious activities, and these systems need constant updates and enhancements to ensure they can detect the latest patterns of financial crime. By reviewing historical data, auditing flagged transactions, and leveraging advanced analytics, institutions can refine their models to enhance the accuracy of suspicious activity detection. This could involve recalibrating risk thresholds, revising criteria for what constitutes suspicious behavior, or incorporating machine learning technologies to improve the prediction and identification of risks.

Training and development are also pivotal to continuous improvement in KYT. As criminal behavior becomes more sophisticated, so too must the knowledge and skills of the employees responsible for monitoring and investigating transactions. Ongoing training ensures that staff are up-to-date on the latest regulations, trends in financial crime, and advancements in technology used for monitoring transactions. Additionally, keeping employees informed about emerging risks, such as new money laundering schemes or changing regulations, allows them to make more informed decisions and respond more effectively when suspicious activity is detected.

Another aspect of continuous improvement in KYT is the integration of feedback from audits and regulatory inspections. Internal audits provide an opportunity to evaluate the effectiveness of the KYT processes, identify weaknesses, and suggest improvements. Similarly, regulatory bodies and external assessments can offer valuable insights into areas where the institution may need to adjust its procedures or enhance its compliance framework. Institutions should implement corrective actions based on audit findings and regulatory feedback to ensure that the KYT system remains robust and compliant with industry standards.

As regulations around anti-money laundering (AML) and counter-terrorism financing (CTF) laws continue to evolve, institutions must ensure that their KYT programs are flexible enough to accommodate new rules, guidelines, and technologies. This requires staying engaged with industry trends, participating in regulatory consultations, and

adjusting internal policies as necessary. By doing so, financial institutions can ensure that their KYT processes remain up-to-date and capable of effectively detecting illicit activities.

Lastly, fostering a culture of compliance is vital for the long-term success of continuous improvement in KYT. Organizations should create an environment where compliance is viewed as an integral part of daily operations, not just as a regulatory obligation. Open communication, transparency, and a strong commitment to ethical practices help ensure that employees understand the importance of effective KYT measures and are empowered to take action when needed.

In summary, continuous improvement in KYT is about maintaining a proactive approach to managing risks and compliance. This involves regularly updating monitoring systems, providing ongoing training for staff, incorporating feedback from audits and regulatory bodies, and adapting to changes in the financial crime landscape. By committing to continuous improvement, financial institutions can better protect themselves from risks, comply with regulations, and contribute to the broader effort of combating money laundering and terrorism financing.

CONCLUSION

PayNox is committed to maintaining a robust transaction monitoring framework that aligns with Bulgarian AML laws, EU directives, and FATF recommendations. By implementing advanced analytics, real-time screening, and strict compliance protocols, PayNox aims to prevent financial crime, protect stakeholders, and uphold the integrity of its platform.

This KYT Policy will be regularly updated to reflect regulatory changes and evolving risks in financial crime prevention.