

Customer Due Diligence

Due Diligence Review Unit

Acceptable Risk is the level of risk that an organization is willing to accept in order to achieve its objectives, it involves weighing the potential benefits against the potential costs and taking steps to mitigate or manage the risks, in the context of Customer Due Diligence, acceptable risk refers to the level of risk that a financial institution is willing to accept when dealing with a customer, this can include the risk of money laundering, terrorist financing, or other illicit activities, for example, a financial institution may consider a customer to be high risk if they are from a country with a high risk of money laundering, or if they have a history of suspicious transactions, in this case, the financial institution may decide to implement additional due diligence measures to mitigate the risk, such as conducting more frequent monitoring of the customer's transactions, or requiring additional identification and verification documents.

AML/CFT stands for Anti-Money Laundering and Combating the Financing of Terrorism, it refers to the laws, regulations, and procedures that are put in place to prevent and detect money laundering and terrorist financing activities, AML/CFT regulations require financial institutions to implement due diligence measures to identify and verify the identity of their customers, and to report suspicious transactions to the relevant authorities, for example, a financial institution may be required to conduct customer due diligence on all new customers, and to monitor their transactions on an ongoing basis to detect and report any suspicious activity.

Beneficial Owner refers to the individual or individuals who ultimately own or control a customer, this can include the owner of a company, or the individual who has control over a trust or other legal entity, in the context of Customer Due Diligence, identifying the beneficial owner is an important step in verifying the identity of a customer, and in assessing the risk that they pose, for example, a financial institution may require a customer to provide identification and verification documents for the beneficial owner, such as a passport or driver's license, and to provide information about the beneficial owner's business activities and sources of funds.

Customer Due Diligence is the process of verifying the identity of a customer, and assessing the risk that they pose, this involves gathering information about the customer, such as their name, address, and date of birth, and verifying this information through various means, such as checking identification documents, or conducting searches of public databases, for example, a financial institution may conduct customer due diligence on a new customer by requiring them to provide identification and verification documents, such as a passport or driver's license, and by conducting a search of public databases to verify the customer's identity and business activities.

Customer Risk Assessment is the process of evaluating the risk that a customer poses to a financial institution, this involves considering various factors, such as the customer's business activities, their country of origin, and their history of suspicious transactions, for example, a financial institution may consider a customer to be high risk if they are from a country with a high risk of money laundering, or if they have a

history of suspicious transactions, in this case, the financial institution may decide to implement additional due diligence measures to mitigate the risk, such as conducting more frequent monitoring of the customer's transactions.

Due Diligence Review Unit refers to a team or department within a financial institution that is responsible for conducting due diligence reviews on customers, this involves verifying the identity of customers, and assessing the risk that they pose, the Due Diligence Review Unit may also be responsible for monitoring customer transactions on an ongoing basis, and for reporting suspicious activity to the relevant authorities, for example, a financial institution may have a Due Diligence Review Unit that is responsible for conducting customer due diligence on all new customers, and for monitoring their transactions on an ongoing basis to detect and report any suspicious activity.

Enhanced Due Diligence is a more extensive and detailed form of due diligence that is required for higher risk customers, this may involve gathering additional information about the customer, such as their business activities and sources of funds, and verifying this information through various means, such as conducting site visits, or reviewing financial statements, for example, a financial institution may require enhanced due diligence for a customer who is from a country with a high risk of money laundering, or who has a history of suspicious transactions.

Financial Action Task Force is an inter-governmental body that is responsible for setting standards and promoting effective implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, and other related threats to the integrity of the international financial system, the Financial Action Task Force issues recommendations and guidelines for countries to follow in order to prevent and detect money laundering and terrorist financing activities.

Know Your Customer is a term that refers to the process of verifying the identity of a customer, and understanding their business activities and needs, this involves gathering information about the customer, such as their name, address, and date of birth, and verifying this information through various means, such as checking identification documents, or conducting searches of public databases, for example, a financial institution may conduct know your customer checks on a new customer by requiring them to provide identification and verification documents, such as a passport or driver's license.

Money Laundering Reporting Officer is a person who is designated by a financial institution to be responsible for reporting suspicious transactions to the relevant authorities, this person is typically responsible for receiving and reviewing reports of suspicious activity from employees, and for determining whether or not to report the activity to the authorities, for example, a financial institution may have a Money Laundering Reporting Officer who is responsible for reviewing reports of suspicious transactions, and for reporting any suspicious activity to the relevant authorities.

Politically Exposed Person is a term that refers to an individual who holds a prominent public position or function, such as a head of state, or a senior government official, these individuals are considered to be higher risk, as they may be more susceptible to corruption, or may have access to large amounts of funds, for example, a financial institution may consider a customer to be a politically exposed person if they are a senior government official, or if they have a close relationship with a senior government official.

Regular Review is the process of periodically reviewing and updating customer due diligence information, this involves verifying that the customer's information is still current and accurate, and assessing whether or not the customer's risk profile has changed, for example, a financial institution may conduct regular reviews of customer due diligence information on an annual basis, or when the customer's circumstances change, such as when they change their business activities or move to a new country.

Risk-Based Approach is a term that refers to the process of assessing the risk that a customer poses, and adjusting the level of due diligence accordingly, this involves considering various factors, such as the customer's business activities, their country of origin, and their history of suspicious transactions, for example, a financial institution may consider a customer to be high risk if they are from a country with a high risk of money laundering, or if they have a history of suspicious transactions, in this case, the financial institution may decide to implement additional due diligence measures to mitigate the risk.

Sanctions Screening is the process of checking a customer's name against lists of individuals and entities that are subject to sanctions, such as those imposed by the United Nations or the European Union, this involves using specialized software to screen the customer's name against these lists, and to identify any potential matches, for example, a financial institution may conduct sanctions screening on a new customer by using specialized software to check their name against lists of sanctioned individuals and entities.

Simplified Due Diligence is a less extensive and detailed form of due diligence that is required for lower risk customers, this may involve gathering less information about the customer, and verifying this information through fewer means, such as checking identification documents, or conducting searches of public databases, for example, a financial institution may require simplified due diligence for a customer who is from a low risk country, and who has a low risk business activity.

Suspicious Activity Report is a report that is filed with the relevant authorities when a financial institution suspects that a customer is engaging in suspicious activity, such as money laundering or terrorist financing, this report typically includes information about the customer, the suspicious activity, and the reasons why the activity is suspicious, for example, a financial institution may file a suspicious activity report if a customer is conducting a large number of transactions in a short period of time, or if a customer is sending money to a country with a high risk of money laundering.

Transaction Monitoring is the process of monitoring a customer's transactions on an ongoing basis to detect and report any suspicious activity, this involves using specialized software to review the customer's transactions, and to identify any patterns or anomalies that may indicate suspicious activity, for example, a financial institution may conduct transaction monitoring on a customer by using specialized software to review their transactions, and to identify any suspicious activity, such as a large number of transactions in a short period of time.

Ultimate Beneficial Owner is the individual or individuals who ultimately own or control a customer, this can include the owner of a company, or the individual who has control over a trust or other legal entity, in the context of Customer Due Diligence, identifying the ultimate beneficial owner is an important step in verifying the identity of a customer, and in assessing the risk that they pose, for example, a financial institution may require a customer to provide identification and verification documents for the ultimate

beneficial owner, such as a passport or driver's license.

Verification is the process of confirming the accuracy of customer due diligence information, this involves checking the customer's information against various sources, such as identification documents, or public databases, for example, a financial institution may verify a customer's identity by checking their passport or driver's license, or by conducting a search of public databases to confirm their address and date of birth.

Watch List is a list of individuals and entities that are subject to sanctions, or that have been identified as being high risk, this list is typically used to screen customers against, and to identify any potential matches, for example, a financial institution may use a watch list to screen a new customer's name against lists of sanctioned individuals and entities, and to identify any potential matches.

Anti-Money Laundering Directive is a directive that is issued by the European Union to prevent and detect money laundering activities, this directive requires financial institutions to implement due diligence measures to identify and verify the identity of their customers, and to report suspicious transactions to the relevant authorities, for example, a financial institution may be required to conduct customer due diligence on all new customers, and to monitor their transactions on an ongoing basis to detect and report any suspicious activity.

Customer Identification Program is a program that is implemented by a financial institution to identify and verify the identity of its customers, this program typically includes procedures for gathering customer information, verifying the accuracy of this information, and monitoring customer transactions on an ongoing basis, for example, a financial institution may have a customer identification program that requires customers to provide identification and verification documents, such as a passport or driver's license.

Due Diligence Checklist is a list of items that are used to conduct due diligence on a customer, this checklist typically includes items such as verifying the customer's identity, assessing their risk profile, and monitoring their transactions on an ongoing basis, for example, a financial institution may use a due diligence checklist to conduct customer due diligence on a new customer, and to ensure that all necessary steps are taken to verify their identity and assess their risk profile.

Financial Intelligence Unit is a unit that is responsible for receiving and analyzing reports of suspicious transactions, and for investigating and pursuing money laundering and terrorist financing activities, for example, a financial institution may have a financial intelligence unit that is responsible for receiving and reviewing reports of suspicious transactions, and for investigating and pursuing money laundering and terrorist financing activities.

Know Your Customer Policy is a policy that is implemented by a financial institution to verify the identity of its customers, and to understand their business activities and needs, this policy typically includes procedures for gathering customer information, verifying the accuracy of this information, and monitoring customer transactions on an ongoing basis, for example, a financial institution may have a know your customer policy that requires customers to provide identification and verification documents, such as a passport or driver's license.

Money Laundering is the process of concealing or disguising the source of funds that are derived from illicit

activities, such as drug trafficking or terrorist financing, this can involve using various techniques, such as structuring transactions, or using shell companies to hide the true ownership of the funds, for example, a person may launder money by depositing cash into a bank account, and then using the funds to purchase a legitimate business or asset.

Risk Assessment is the process of evaluating the risk that a customer poses, and adjusting the level of due diligence accordingly, this involves considering various factors, such as the customer's business activities, their country of origin, and their history of suspicious transactions, for example, a financial institution may consider a customer to be high risk if they are from a country with a high risk of money laundering, or if they have a history of suspicious transactions, in this case, the financial institution may decide to implement additional due diligence measures to mitigate the risk.

Sanctions Compliance is the process of ensuring that a financial institution is in compliance with sanctions that are imposed by governments or international organizations, this involves screening customers against lists of sanctioned individuals and entities, and reporting any matches to the relevant authorities, for example, a financial institution may conduct sanctions screening on a new customer by using specialized software to check their name against lists of sanctioned individuals and entities.

Simplified Customer Due Diligence is a less extensive and detailed form of due diligence that is required for lower risk customers, this may involve gathering less information about the customer, and verifying this information through fewer means, such as checking identification documents, or conducting searches of public databases, for example, a financial institution may require simplified customer due diligence for a customer who is from a low risk country, and who has a low risk business activity.

Terrorist Financing is the process of providing financial support to terrorist organizations or activities, this can involve using various techniques, such as donating funds, or providing goods and services, for example, a person may provide financial support to a terrorist organization by sending them money, or by providing them with goods and services, such as weapons or explosives.

Transaction Risk Assessment is the process of evaluating the risk that a transaction poses, and adjusting the level of due diligence accordingly, this involves considering various factors, such as the type of transaction, the amount of funds involved, and the parties to the transaction, for example, a financial institution may consider a transaction to be high risk if it involves a large amount of funds, or if it involves a party that is from a country with a high risk of money laundering.

Ultimate Beneficial Owner Identification is the process of identifying the individual or individuals who ultimately own or control a customer, this can include the owner of a company, or the individual who has control over a trust or other legal entity, for example, a financial institution may require a customer to provide identification and verification documents for the ultimate beneficial owner, such as a passport or driver's license.

Verification of Identity is the process of confirming the accuracy of customer due diligence information, this involves checking the customer's information against various sources, such as identification documents, or public databases, for example, a financial institution may verify a customer's identity by checking their

passport or driver's license, or by conducting a search of public databases to confirm their address and date of birth.

Watch List Screening is the process of checking a customer's name against lists of individuals and entities that are subject to sanctions, or that have been identified as being high risk, this involves using specialized software to screen the customer's name against these lists, and to identify any potential matches, for example, a financial institution may conduct watch list screening on a new customer by using specialized software to check their name against lists of sanctioned individuals and entities.

Anti-Terrorist Financing is a set of laws, regulations, and procedures that are put in place to prevent and detect terrorist financing activities, this includes requirements for financial institutions to implement due diligence measures to identify and verify the identity of their customers, and to report suspicious transactions to the relevant authorities, for example, a financial institution may be required to conduct customer due diligence on all new customers, and to monitor their transactions on an ongoing basis to detect and report any suspicious activity.

Customer Acceptance Policy is a policy that is implemented by a financial institution to determine whether or not to accept a new customer, this policy typically includes procedures for gathering customer information, verifying the accuracy of this information, and assessing the risk that the customer poses, for example, a financial institution may have a customer acceptance policy that requires customers to provide identification and verification documents, such as a passport or driver's license.

Due Diligence Procedure is a procedure that is implemented by a financial institution to conduct due diligence on a customer, this procedure typically includes steps such as verifying the customer's identity, assessing their risk profile, and monitoring their transactions on an ongoing basis, for example, a financial institution may have a due diligence procedure that requires customers to provide identification and verification documents, such as a passport or driver's license.

Financial Institution is an organization that provides financial services, such as banking, securities, or insurance, for example, a bank, a brokerage firm, or an insurance company.

High Risk Customer is a customer who poses a higher risk of money laundering, terrorist financing, or other illicit activities, this can include customers who are from countries with a high risk of money laundering, or who have a history of suspicious transactions, for example, a financial institution may consider a customer to be high risk if they are from a country with a high risk of money laundering, or if they have a history of suspicious transactions.

Identity Verification is the process of confirming the accuracy of customer due diligence information, this involves checking the customer's information against various sources, such as identification documents, or public databases, for example, a financial institution may verify a customer's identity by checking their passport or driver's license, or by conducting a search of public databases to confirm their address and date of birth.

Know Your Customer Requirements are the requirements that are imposed on financial institutions to verify the identity of their customers, and to understand their business activities and needs, this includes

requirements for gathering customer information, verifying the accuracy of this information, and monitoring customer transactions on an ongoing basis, for example, a financial institution may be required to conduct customer due diligence on all new customers, and to monitor their transactions on an ongoing basis to detect and report any suspicious activity.

Money Laundering Regulations are the regulations that are imposed on financial institutions to prevent and detect money laundering activities, this includes requirements for implementing due diligence measures to identify and verify the identity of customers, and for reporting suspicious transactions to the relevant authorities, for example, a financial institution may be required to conduct customer due diligence on all new customers, and to monitor their transactions on an ongoing basis to detect and report any suspicious activity.

Politically Exposed Person Risk is the risk that a customer poses because of their prominent public position or function, this can include the risk of corruption, or the risk of being used to launder money or finance terrorism, for example, a financial institution may consider a customer to be a politically exposed person if they are a senior government official, or if they have a close relationship with a senior government official.

Regulatory Requirements are the requirements that are imposed on financial institutions by regulatory bodies, such as the Financial Action Task Force, or the European Union, these requirements can include requirements for implementing due diligence measures to identify and verify the identity of customers, and for reporting suspicious transactions to the relevant authorities, for example, a financial institution may be required to conduct customer due diligence on all new customers, and to monitor their transactions on an ongoing basis to detect and report any suspicious activity.

Risk Management is the process of identifying, assessing, and mitigating risks, this can include risks such as money laundering, terrorist financing, or other illicit activities, for example, a financial institution may have a risk management process that includes identifying and assessing the risk that a customer poses, and implementing due diligence measures to mitigate that risk.

Sanctions List is a list of individuals and entities that are subject to sanctions, this list is typically used to screen customers against, and to identify any potential matches, for example, a financial institution may use a sanctions list to screen a new customer's name against lists of sanctioned individuals and entities.

Simplified Due Diligence Procedure is a procedure that is implemented by a financial institution to conduct simplified due diligence on a customer, this procedure typically includes steps such as gathering less information about the customer, and verifying this information through fewer means, such as checking identification documents, or conducting searches of public databases, for example, a financial institution may have a simplified due diligence procedure that requires customers to provide identification and verification documents, such as a passport or driver's license.

Terrorist Financing Regulations are the regulations that are imposed on financial institutions to prevent and detect terrorist financing activities, this includes requirements for implementing due diligence measures to identify and verify the identity of customers, and for reporting suspicious transactions to the relevant authorities, for example, a financial institution may be required to conduct customer due diligence on all

new customers, and to monitor their transactions on an ongoing basis to detect and report any suspicious activity.

Transaction Monitoring System is a system that is used by a financial institution to monitor customer transactions on an ongoing basis, this system typically includes software that is used to review customer transactions, and to identify any suspicious activity, for example, a financial institution may have a transaction monitoring system that includes software that is used to review customer transactions, and to identify any suspicious activity, such as a large number of transactions in a short period of time.

Ultimate Beneficial Owner Verification is the process of verifying the identity of the individual or individuals who ultimately own or control a customer, this can include the owner of a company, or the individual who has control over a trust or other legal entity, for example, a financial institution may require a customer to provide identification and verification documents for the ultimate beneficial owner, such as a passport or driver's license.

Verification of Address is the process of confirming the accuracy of a customer's address, this involves checking the customer's address against various sources, such as identification documents, or public databases, for example, a financial institution may verify a customer's address by checking their passport or driver's license, or by conducting a search of public databases to confirm their address.

Watch List Maintenance is the process of maintaining and updating lists of individuals and entities that are subject to sanctions, or that have been identified as being high risk, this involves adding or removing names from the list, and updating the list to reflect any changes, for example, a financial institution may maintain a watch list of sanctioned individuals and entities, and update the list on a regular basis to reflect any changes.

Anti-Money Laundering Software is software that is used by financial institutions to prevent and detect money laundering activities, this software typically includes tools for customer due diligence, transaction monitoring, and reporting suspicious activity, for example, a financial institution may use anti-money laundering software to conduct customer due diligence on new customers, and to monitor their transactions on an ongoing basis to detect and report any suspicious activity.

Customer Due Diligence Software is software that is used by financial institutions to conduct customer due diligence, this software typically includes tools for gathering customer information, verifying the accuracy of this information, and assessing the risk that the customer poses, for example, a financial institution may use customer due diligence software to conduct customer due diligence on new customers, and to assess the risk that they pose.

Financial Crime is a term that refers to crimes that are related to finance, such as money laundering, terrorist financing, or securities fraud, for example, a person may commit a financial crime by laundering money, or by engaging in insider trading.

Financial Institution Regulations are the regulations that are imposed on financial institutions to prevent and detect financial crimes, such as money laundering, terrorist financing, or securities fraud, for example, a financial institution may be required to implement due diligence measures to identify and verify the identity

of customers, and to report suspicious transactions to the relevant authorities.

Identity Verification Software is software that is used to verify the identity of customers, this software typically includes tools for checking identification documents, and for conducting searches of public databases, for example, a financial institution may use identity verification software to verify the identity of new customers, and to confirm their address and date of birth.

Money Laundering Detection is the process of detecting and reporting suspicious transactions that may be related to money laundering, this involves using various techniques, such as transaction monitoring, and reporting suspicious activity to the relevant authorities, for example, a financial institution may have a money laundering detection system that includes software that is used to review customer transactions, and to identify any suspicious activity.

Regulatory Compliance is the process of ensuring that a financial institution is in compliance with regulatory requirements, such as those related to anti-money laundering, or know your customer, for example, a financial institution may have a regulatory compliance program that includes procedures for implementing due diligence measures, and for reporting suspicious transactions to the relevant authorities.

Risk Assessment Software is software that is used to assess the risk that a customer poses, this software typically includes tools for gathering customer information, and for evaluating the risk that the customer poses, for example, a financial institution may use risk assessment software to assess the risk that a new customer poses, and to determine the level of due diligence that is required.

Sanctions Compliance Software is software that is used to ensure that a financial institution is in compliance with sanctions, this software typically includes tools for screening customers against lists of sanctioned individuals and entities, and for reporting any matches to the relevant authorities, for example, a financial institution may use sanctions compliance software to screen new customers against lists of sanctioned individuals and entities.

Transaction Monitoring Software is software that is used to monitor customer transactions on an ongoing basis, this software typically includes tools for reviewing customer transactions, and for identifying any suspicious activity, for example, a financial institution may use transaction monitoring software to review customer transactions, and to identify any suspicious activity, such as a large number of transactions in a short period of time.

Ultimate Beneficial Owner Identification Software is software that is used to identify the individual or individuals who ultimately own or control a customer, this software typically includes tools for gathering customer information, and for verifying the identity of the ultimate beneficial owner, for example, a financial institution may use ultimate beneficial owner identification software to identify the ultimate beneficial owner of a new customer, and to verify their identity.

Verification of Identity Software is software that is used to verify the identity of customers, this software typically includes tools for checking identification documents, and for conducting searches of public databases, for example, a financial institution may use verification of identity software to verify the identity of new customers, and to confirm their address and date of birth.

Watch List Screening Software is software that is used to screen customers against lists of individuals and entities that are subject to sanctions, or that have been identified as being high risk, this software typically includes tools for searching the lists, and for identifying any potential matches, for example, a financial institution may use watch list screening software to screen new customers against lists of sanctioned individuals and entities.

Anti-Money Laundering Training is training that is provided to employees of financial institutions to prevent and detect money laundering activities, this training typically includes information on the risks of money laundering, and the procedures for implementing due diligence measures, for example, a financial institution may provide anti-money laundering training to its employees on a regular basis, to ensure that they are aware of the risks of money laundering, and know how to implement due diligence measures.

Customer Due Diligence Training is training that is provided to employees of financial institutions to conduct customer due diligence, this training typically includes information on the procedures for gathering customer information, verifying the accuracy of this information, and assessing the risk that the customer poses, for example, a financial institution may provide customer due diligence training to its employees on a regular basis, to ensure that they know how to conduct customer due diligence, and assess the risk that a customer poses.

Financial Crime Prevention is the process of preventing and detecting financial crimes, such as money laundering, terrorist financing, or securities fraud, this involves using various techniques, such as transaction monitoring, and reporting suspicious activity to the relevant authorities, for example, a financial institution may have a financial crime prevention program that includes procedures for implementing due diligence measures, and for reporting suspicious transactions to the relevant authorities.

Identity Verification Training is training that is provided to employees of financial institutions to verify the identity of customers, this training typically includes information on the procedures for checking identification documents, and for conducting searches of public databases, for example, a financial institution may provide identity verification training to its employees on a regular basis, to ensure that they know how to verify the identity of customers.

Money Laundering Reporting is the process of reporting suspicious transactions that may be related to money laundering, this involves using various techniques, such as transaction monitoring, and reporting suspicious activity to the relevant authorities, for example, a financial institution may have a money laundering reporting system that includes software that is used to review customer transactions, and to identify any suspicious activity.

Regulatory Compliance Training is training that is provided to employees of financial institutions to ensure that they are aware of regulatory requirements, and know how to implement procedures to comply with these requirements, for example, a financial institution may provide regulatory compliance training to its employees on a regular basis, to ensure that they are aware of regulatory requirements, and know how to implement procedures to comply with these requirements.

Risk Assessment Training is training that is provided to employees of financial institutions to assess the risk

that a customer poses, this training typically includes information on the procedures for gathering customer information, and for evaluating the risk that the customer poses, for example, a financial institution may provide risk assessment training to its employees on a regular basis, to ensure that they know how to assess the risk that a customer poses.

Sanctions Compliance Training is training that is provided to employees of financial institutions to ensure that they are aware of sanctions, and know how to implement procedures to comply with these sanctions, for example, a financial institution may provide sanctions compliance training to its employees on a regular basis, to ensure that they are aware of sanctions, and know how to implement procedures to comply with these sanctions.

Transaction Monitoring Training is training that is provided to employees of financial institutions to monitor customer transactions on an ongoing basis, this training typically includes information on the procedures for reviewing customer transactions, and for identifying any suspicious activity, for example, a financial institution may provide transaction monitoring training to its employees on a regular basis, to ensure that they know how to review customer transactions, and identify any suspicious activity.

Ultimate Beneficial Owner Identification Training is training that is provided to employees of financial institutions to identify the individual or individuals who ultimately own or control a customer, this training typically includes information on the procedures for gathering customer information, and for verifying the identity of the ultimate beneficial owner, for example, a financial institution may provide ultimate beneficial owner identification training to its employees on a regular basis, to ensure that they know how to identify the ultimate beneficial owner of a customer.

Verification of Identity Training is training that is provided to employees of financial institutions to verify the identity of customers, this training typically includes information on the procedures for checking identification documents, and for conducting searches of public databases, for example, a financial institution may provide verification of identity training to its employees on a regular basis, to ensure that they know how to verify the identity of customers.

Watch List Screening Training is training that is provided to employees of financial institutions to screen customers against lists of individuals and entities that are subject to sanctions, or that have been identified as being high risk, this training typically includes information on the procedures for searching the lists, and for identifying any potential matches, for example, a financial institution may provide watch list screening training to its employees on a regular basis, to ensure that they know how to screen customers against the lists, and identify any potential matches.