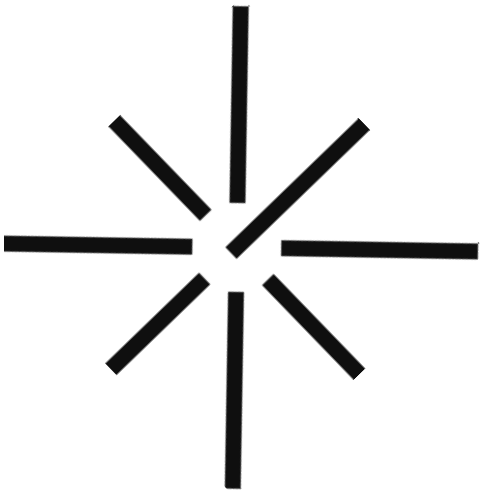
Golden Suisse®



GCB Suisse AG
Schipfe 2
8001 Zürich
Schweiz

www.goldensuisse.com

ANTI-MONEY LAUNDERING & COUNTER TERRORIST FINANCING POLICY

Version 6

Published August 2026 (Amended)

Sensitivity Confidential

Table of Contents

1. Introduction 3
2. Key Definitions 4
3. Scope and Objective 6
4. The Money Laundering Reporting Officer (MLRO) 7
5. Employees screening and Vetting 8
6. Business Wide Risk Assessment 9
7. Risk Appetite Statement 10
8. Risk-Based Approach 13
9. Risk Assessment 14
10. Customer Due Diligence 15
11. Identification of the Customer – natural person 17
12. Enhanced Due Diligence 18
13. Sanction Screening 21
14. Politically Exposed Person (PEP) screening 22
15. Adverse Media Screening and Special Interest Persons (SIP) Screening 25
16. Transaction Monitoring 25
17. Ongoing Monitoring and Client Reviews 26
18. Suspicious Activity Reporting 27
19. The Exit of a Business Relationship 28
20. Training 29
21. Employee Awareness 29
22. Record Keeping 30
ANNEX 31

1. Introduction

The purpose of this process is to establish controls for GCB Suisse AG against Anti-Money Laundering and Counter-Terrorist Financing. It aims to introduce measures that mitigate the risks of money laundering and/or terrorist financing threats, which GCB Suisse AG (hereinafter referred to as "the Company" or Golden Suisse) may encounter as a result of its business activities.

Golden Suisse fully acknowledges that its products and services might be at risk from individuals seeking to launder criminal proceeds or facilitate funds designated for the financing of terrorism. As such, the company is committed to fostering and promoting a compliance culture throughout the firm which underpins the importance of preventing Money Laundering and Terrorist Financing.

The company maintains systems and controls to prevent financial crime that align with the risks inherent in its business and products. Consequently, the Company has developed this AML Program. As part of this program, GCB Suisse AG is obligated to adhere to the following:

- Anti-Money Laundering Act (AMLA) and related ordinances;
- Swiss Criminal Code (SCC);
- Federal Act Prohibiting the Groups “Al-Qaida” and “Islamic State” and Related Organisations, Article 260ter of the Swiss Criminal Code, and other relevant Swiss legislation;
- Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector (Geldwäschereigesetz, GwG);
- Federal Act on the Implementation of International Sanctions (Embargo Act, EmbG, SR 946.231) and the sanctions ordinances issued thereunder;
- Relevant FINMA regulations, guidelines, and circulars.

The Company takes into account the guidance, provisions, and findings contained within:

- Financial Market Supervisory Authority (FINMA) guidelines and circulars;
- Financial Market Supervisory Authority (FINMA) Anti-Money Laundering (AML) Circulars;
- Federal Department of Finance (FDF) regulations and guidance on combating money laundering and terrorist financing;
- Relevant guidance and reports issued by the Financial Action Task Force (FATF) and other international organizations.

2. Key Definitions

Money laundering ("ML") is defined as the process of concealing, disguising, converting, transferring, or removing the proceeds of criminal activity to make them appear legitimate. It involves handling funds or property that are the product of criminal conduct, with the intention of disguising the illicit origins of those funds or property. The primary purpose of money laundering is to enable criminals to enjoy the benefits of their illegal activities without drawing attention to the true source of their funds. Money laundering is a criminal offense under the Anti-Money Laundering Act (AMLA).

Terrorist financing ("TF") refers to the provision, collection, or receipt of funds or other financial resources, with the intention or knowledge that they will be used for the purposes of terrorism. The definition encompasses various activities, including:

1. Directly or indirectly providing funds or financial assistance to individuals, groups, or organizations involved in terrorist activities.

2. Fundraising, collecting, or soliciting money with the knowledge or suspicion that it will be used to support terrorist acts.

3. Possessing, managing, or using money or property with the intent to facilitate acts of terrorism.

Customer/ Client – a person (whether legal or natural); who seeks to form a business relationship; or with whom a business relationship is formed.

Senior management – Company's officers or employees with sufficient seniority, possessing sufficient knowledge of the Company's ML/TF risk exposure, and responsible for taking decisions affecting its risk exposure (i.e. CEO, Board Members).

Financial Crime refers to a variety of illegal activities involving the abuse of financial systems and institutions for criminal purposes. It includes various offenses such as money laundering, fraud, bribery, corruption, terrorist financing, insider trading, tax evasion, and other illicit financial activities.

Financial sanctions are measures imposed by national governments and multinational bodies aimed at influencing the behavior and decisions of other national governments or

non-state actors that may pose a threat to global security or violate international norms. GCB Suisse AG complies with the following sanctions measures:

1. The Swiss State Secretariat for Economic Affairs (SECO) sanctions lists;
2. The European Union's consolidated list of persons, groups, and entities;
3. The United Nations (UN) Security Council consolidated sanctions list;
4. The US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists;
5. The US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) list.

Key stages of money laundering - Money laundering is typically divided into three distinct stages:

- **Placement:** This involves the physical or financial placement of proceeds from criminal activities or illegally obtained funds into financial institutions.

- **Layering:** This stage entails separating these proceeds from their original source by creating layers of transactions intended to conceal the ultimate source and transfer of the funds. For example, illegally obtained funds may be divided into multiple transactions to hide their origin and obscure the connection to the initial entry point.

- **Integration:** Integration involves giving the appearance of legitimacy to the proceeds from criminal activities. Integration schemes reintroduce the illegally obtained funds into the economy as seemingly legitimate funds.

Money Laundering Offence: Pursuant to article 305bis of the Swiss Criminal Code (SCC), the following actions constitute money laundering and are subject to criminal proceedings:

1. Taking steps to obstruct the identification, tracing, or forfeiture of assets that one knows or should assume originate from a felony or qualified tax offense;

2. Committing a predicate offense, felony, or qualified tax offense;

3. The assets originating from such predicate offense could be forfeited;

4. Intentionally committing an act aimed at forfeiting such assets;

5. Knowing or should have known that the assets originate from a predicate offense;

6. Predicate offenses include crimes against property such as misappropriation, fraud, robbery, criminal mismanagement, handling stolen goods, bankruptcy offenses, drug dealing, bribery, and evasion of indirect taxes, including stamp duties, withholding tax, VAT, customs duties, etc.

7. Engaging in or participating in an arrangement that the client knows or suspects facilitates the acquisition, retention, use, or control of criminal property by or on behalf of another person (section 328); or
8. Acquiring, using, or possessing criminal property (section 329);

9. Participating in an arrangement that facilitates the concealment, removal from the jurisdiction, transfer to nominees, or any other retention or control of terrorist property (section 18, Terrorism Act 2000).

3. Scope and Objective

The policy outlines how GCB Suisse AG will manage the risks associated with money laundering and ensure consistency across the company.

This policy provides comprehensive guidance to employees of the company on addressing anti-money laundering issues.

All employees, directors, officers, and affiliated agents are required to adhere to this policy. Failure to comply may result in disciplinary and/or legal consequences.

This AML policy, along with other existing AML controls, aims to achieve the following:

1. Define the Due Diligence processes that the Company’s Compliance Team must follow for proper customer onboarding.

2. Identify ML and TF risks inherent to the company's business through established customer risk assessment procedures.

3. Define the Company’s risk appetite statement for each member to adhere to in their respective duties.

4. Implement procedures for screening customers.

5. Identify suspicious transactions and define appropriate actions for reporting them.

6. Appoint a MLRO responsible for AML Compliance.

7. Provide AML&CTF training to employees.

8. Implement internal record-keeping requirements.

The company must ensure that its internal controls and procedures effectively identify, assess, and manage ML/TF risks.

The AML policy should undergo review at least annually and whenever there are changes in legislative requirements, modifications in the company's activities, results of the BWRA, or significant events.

The MLRO is responsible for monitoring compliance with this AML policy. All employees must read the policy and confirm their understanding in writing. Additionally, new employees must complete AML and Sanctions training before starting work, and existing employees must undergo AML training annually.

4. The Money Laundering Reporting Officer (MLRO)

GCB Suisse AG clearly outlines the roles and responsibilities of all individuals overseeing the firm’s AML/CTF strategy and ensuring compliance with all AML/CTF requirements.

The policy will be communicated to all staff during their onboarding process. Updates will be communicated via email from the MLRO. In relation to training requirements, administrative staff (e.g., janitors, receptionists, maintenance personnel) who do not handle financial transactions or sensitive customer information may not require AML training. Similarly, software developers based abroad who are not directly involved in financial operations or customer interactions, unless working on systems related to AML compliance, may also be exempt from AML training.

Golden Suisse’s CEO Chief Compliance Officer is the company’s Money Laundering Reporting Officer (MLRO) responsible for the following:

1. Ensuring that the firm’s AML/CTF policies, procedures, and controls are appropriately designed and implemented to mitigate the firm’s exposure to Money Laundering and Terrorist Financing.
2. Participating in the decision-making process regarding the firm’s AML/CTF strategy and taking ownership of the risk-based approach.
3. Involvement in the development of the firm’s policies, procedures, and controls, as well as approving them.
4. Understanding the level of Money Laundering and Terrorist Financing risk to which the firm is exposed.
5. Ensuring that the firm fulfills its obligations under the Anti-Money Laundering Act, Federal Act on the Suppression of Terrorism, and other relevant Swiss regulations.

6. Implement Business Risk Assessment for each activity undertaken by the company,
7. Incorporate legal and regulatory requirements into company policies and procedures,
8. Establish a monitoring system for suspicious transactions to enable reporting investigation, documentation, and handing off to the authorities,
9. Carry out regular risk assessments and advise on actions to be taken,
10. Promote a compliance culture across Golden Suisse,
11. Serve as the company's liaison with the regulator.
12. Handling communication between the Company and relevant authorities.
13. Receiving, analyzing, and submitting internal suspicious activity reports.
14. Approving Politically Exposed Persons (PEPs).
15. Approving higher-risk customers.
16. Delivering training sessions.

5. Employees screening and Vetting

It is crucial that GCB Suisse AG is vigilant about the possibility of any of its managers, internal or external staff (employees) engaging in ML/TF activities or assisting individuals outside the company in such activities.

To prevent and detect any potential misconduct by an employee, the company policy includes rigorous processes for recruiting new staff and monitoring all relevant staff activities.

GCB Suisse AG assesses the risk of money laundering or terrorism financing associated with individual positions within the company and conducts appropriate due diligence and screening of employees in each case.

Employees undergo screening upon onboarding and at regular intervals during their employment with the company. Employee screening involves evaluating:

- The skills, knowledge, and expertise necessary for the effective performance of their duties.

- The behavior and integrity of the individual.

All employees receive training to recognize and report suspicious activities. They also undergo regular training on the laws pertaining to Anti-Money Laundering and Counter-Terrorist Financing.

6. Business Wide Risk Assessment

To implement a comprehensive risk-based approach, the company must conduct a thorough analysis of its exposure to ML/TF risks. Therefore, senior management at GCB Suisse AG recognizes the importance of conducting a firm-wide risk assessment to identify and evaluate ML/TF risks relevant to the business.

This assessment ensures that ML/TF risks are adequately identified and continually monitored, allowing the company to implement proportionate measures to effectively manage these risks.

The Business-Wide Risk Assessment (BWRA) must consider risks arising from the following categories:

1. Jurisdictional Risk.
2. Customer Risk.
3. Product/Service Risk.
4. Transaction Volume Risk.
5. Delivery Channel Risk.

The company conducted a Business-Wide Risk Assessment (BWRA) considering the inherent risks of the business and their potential impact and likelihood. Subsequently, the company evaluated appropriate controls to mitigate these risks and established an acceptable risk level or risk appetite. This process helps clearly identify acceptable relationships and those considered risky, where identified risks cannot be sufficiently mitigated through existing controls. As a result, relationships deemed unacceptable to the company are promptly identified. This comprehensive approach ensures effective mitigation of any remaining risk after the risk assessment.

All inherent risks in the business must be identified and mitigated accordingly. An overall residual risk to the firm’s business must be developed, and controls and resources allocated where most needed to mitigate ML/TF risks. More resources and risk-mitigating measures must be allocated to areas with the highest identified risks.

The Management Board of GCB Suisse AG is informed about the results of the firm-wide risk assessment. The compliance team will record in the BWRA the number of High-Risk clients, the number of customers using high-risk products, the number of transactions

performed in high-risk countries, and the number of customers in different risk groups (low, moderate, high).

The BWRA must be reviewed annually or more frequently if triggered by an event.

7. Risk Appetite Statement

GCB Suisse AG is dedicated to combatting financial crime and ensuring that its products are not utilized for the purposes of money laundering, terrorist financing, or fraudulent activities. The company upholds strict and transparent standards and continually enhances its internal processes to ensure compliance with relevant laws and regulations.

The risk appetite applies to all employees, customers, products, and activities of the company. The company must adhere to the Risk Appetite Statement in cases where concerns or issues arise regarding GCB Suisse AG's conduct, its customers, products, or countries of operation.

The company has zero tolerance for:

1. Establishing or maintaining business relationships with clients from sanctioned countries or activities.

2. Maintaining business relationships with customers attempting to initiate or receive transactions from prohibited jurisdictions.

For risk-management purposes, the Company classifies non-acceptance jurisdictions into tiers based on the nature of the underlying Swiss sanctions measure. This classification determines whether a documented case-by-case exception under Section 7.1 below may be considered for a specific client.

Tier 1 – Comprehensive/Sectoral Sanctions Jurisdictions. The Company does not accept, and will not grant any exception for, customers resident in the following jurisdictions, which are subject to a comprehensive or broad sectoral Swiss sanctions ordinance:

1. Belarus
2. Crimea and Sevastopol
3. Iran
4. Myanmar/Burma
5. North Korea
6. Russia (excluding Crimea and Sevastopol)
7. Syria

Tier 2 – Targeted Sanctions Jurisdictions. The Company does not accept customers resident in the following jurisdictions by default. These jurisdictions are subject to a Swiss sanctions ordinance that targets specific named individuals, entities, or a narrow sector (rather than the general population), so a documented case-by-case exception may be granted strictly in accordance with Section 7.1 below:

1. Afghanistan
2. Burundi
3. Central African Republic
4. Democratic Republic of the Congo
5. Guatemala
6. Guinea
7. Guinea-Bissau
8. Haiti
9. Iraq
10. Lebanon
11. Libya
12. Mali
13. Moldova
14. Nicaragua
15. Somalia
16. South Sudan
17. Sudan
18. Venezuela
19. Yemen
20. Zimbabwe

FATF Enhanced-Monitoring Jurisdictions. The following jurisdictions carry no Swiss sanctions ordinance but are currently identified by the Financial Action Task Force as subject to increased monitoring for strategic AML/CFT deficiencies. They are treated as Tier 2 for acceptance and exception purposes:

1. Bosnia and Herzegovina
2. Laos

This list must be reviewed no less than semi-annually, and immediately upon any new or amended SECO sanctions ordinance or FATF plenary outcome affecting a jurisdiction, to remain aligned with the SECO Consolidated Sanctions List, the UN Security Council Consolidated List, the EU Consolidated List, and the FATF list of jurisdictions under increased monitoring. The MLRO is responsible for conducting and documenting each review by reference to: (i) SECO's list of sanctions ordinances (seco.admin.ch); (ii) the

UN Security Council Consolidated List; (iii) the EU Consolidated List; and (iv) the outcomes of each FATF plenary. Each review must be recorded in a dated compliance log retained for audit purposes, confirming the sources checked, any changes identified, and the resulting amendments to this Section 7.

The company maintains a strict policy of zero tolerance towards any violations of financial crime laws and regulations within its business operations.

Moreover, the company strictly prohibits engaging with any individual or entity who is subject to international sanctions or embargoes, or who is connected to such a person or entity, regardless of the jurisdiction tier above. It is essential for the company to fully comply with all sanctions requirements; this prohibition is absolute and is not subject to the case-by-case exception process described in Section 7.1.

7.1 Case-by-Case Exception Assessment (Tier 2 and FATF Enhanced-Monitoring Jurisdictions Only)

Residence in a Tier 2 or FATF enhanced-monitoring jurisdiction does not, by itself, indicate a money laundering, terrorist financing, or sanctions risk — for example, a Swiss national who relocates for personal or family reasons while maintaining Swiss-sourced wealth. Accordingly, the MLRO may approve a documented exception to the default non-acceptance position for a specific client, on a case-by-case basis, subject to all of the following conditions being met and evidenced in the client file:

1. The client, and each underlying beneficial owner, is not a Politically Exposed Person, government official, military official, or state-owned or state-affiliated entity of the jurisdiction concerned.
2. Neither the client nor any underlying beneficial owner, nor any known close associate or family member, is named on the SECO Consolidated Sanctions List, the UN Security Council Consolidated List, or the EU Consolidated List.
3. The client's source of wealth and source of funds are independently verified and demonstrably unconnected to the jurisdiction's underlying risk drivers (including armed conflict, extractive industries, government contracts, or the arms trade).
4. The client's connection to the jurisdiction is personal, family-related, or incidental (such as residence or marriage) rather than commercial, governmental, or political.
5. No transaction is to be sent to, received from, or conducted for the benefit of any government body, state-owned entity, or sanctioned person or entity located in or connected to the jurisdiction, other than the client's ordinary personal living expenses.

Exceptions are granted through the following process:

1. The relationship manager or Compliance submits a written exception request to the MLRO, together with the complete KYC/EDD file and sanctions screening results.
2. The MLRO assesses the request against the conditions above and issues a dated, written decision setting out the rationale, which is retained permanently in the client file.
3. An approved exception is subject to Enhanced Due Diligence, a minimum annual KYC refresh (or more frequently if warranted), and ongoing transaction monitoring calibrated to the jurisdiction's risk drivers.
4. The MLRO must immediately reassess any approved exception upon a change in the client's circumstances, a new or amended sanctions ordinance or FATF listing affecting the jurisdiction, or any adverse information concerning the client.
5. All exceptions granted, declined, or withdrawn are logged in an Exceptions Register, which is reviewed at each semi-annual jurisdiction review under this Section 7 and made available to auditors and regulators upon request.

No exception may be granted, under any circumstances, for a Tier 1 jurisdiction, or for any client, transaction, or connected party implicated in the zero-tolerance prohibitions above.

8. Risk-Based Approach

GCB Suisse AG is required to adopt a risk-based approach to identify, monitor, manage, and mitigate the risks associated with the company being used for ML/TF.

This approach aims to identify the most cost-effective and proportionate way to manage and mitigate the risks posed to the company.

The rationale behind the company's application of the risk-based approach is not to deviate from CDD measures where the risk of ML/TF is low, but rather to provide flexibility to vary the extent of the application of CDD measures depending on the level of identified risks.

The risk-based approach enables senior management to customize systems and controls to specific business needs, thereby focusing resources more effectively where needed.

A risk-based approach requires GCB Suisse AG to undertake the following steps:

1. Identify ML/TF risks relevant to the company.
2. Assess the risks presented, particularly regarding:
    a. Customers and any underlying beneficial owners

   b. Products or services
   c. Acquisition channels (inbound vs. outbound)
   d. Geographical areas of operation
3. Design and implement controls to manage and mitigate these assessed risks, considering the company's risk appetite.
4. Monitor and enhance the effective operation of these controls and appropriately document the actions taken and the reasons behind them.

The company regularly undertakes appropriate measures, proportionate to the nature and size of its operations, to identify and evaluate the risks of money laundering and terrorist financing arising from its activities or business. This includes considering risk factors such as customer profiles, geographical locations, delivery channels, and any national or supranational risk assessments related to money laundering and terrorist financing risks.

During the onboarding process of a business relationship, as well as on an ongoing basis, a risk assessment of the applicant's business, including beneficial ownership, will be conducted based on the following risk criteria:

1. Customer Risk
2. Product Risk
3. Geographical/Country Risk
4. Channel Risk

The resulting risk category will determine:

1. Acceptance or rejection of the business relationship
2. Type of due diligence conducted
3. Frequency of ongoing monitoring.

9. Risk Assessment

GCB Suisse AG assesses AML/CTF risks by implementing a risk-based approach and considering national and supranational risk assessments, as well as recommendations and guidelines from organizations such as the Financial Action Task Force (FATF), European Banking Authority (EBA), and other relevant international and local laws and regulations.

In compliance with Swiss regulations, the company conducts regular risk assessments to evaluate all Money Laundering and Terrorist Financing risks associated with its business operations.

The company has developed a Customer Risk Assessment (CRA) framework to assess inherent risks across its consumer clients. This includes internal procedures and processes to conduct individual ML/TF risk assessments and categorize customers into specific risk categories based on factors such as customer type, activity frequency, relationship history, country of residence, and offered products.

Areas assessed to determine the company’s AML vulnerabilities include risks posed by customers, products and services offered, geographical areas of operation, transaction volume and complexity, and delivery channels used.

Appropriate due diligence is conducted before establishing a business relationship with a client, with the level of due diligence determined by the client's inherent risk rating and ongoing monitoring requirements.

Clients undergo a Customer Risk Assessment (CRA) during onboarding and at regular intervals thereafter. Risk levels (Low, Moderate, or High) are assigned based on various factors, with different review frequencies applied accordingly.

Changes in a client's circumstances or risk factors may lead to a reassessment of their risk level, with due diligence re-requested for verification purposes.

Any significant changes in risk types during the client relationship, such as adverse media discoveries, ownership structure changes, or unusual behavior, trigger a re-review of the customer's inherent risk assessment.

In cases of suspicious behavior, an Unusual Activity Report is completed and submitted to relevant issuing institution, with a Suspicious Activity Report (SAR) filed with the Money Laundering Reporting Office Switzerland (MROS) if suspicions are justified.

10. Customer Due Diligence

One of the key requirements for preventing money laundering is the implementation of customer-related due diligence or Know Your Customer (KYC) processes. These obligations include identifying the customer and any persons acting on their behalf, determining the beneficial owner, gathering information on the purpose and intended nature of the business relationship, assessing any politically exposed person (PEP) status, and continuously monitoring the business relationship.

The existing Customer Due Diligence Procedures at GCB Suisse AG enable the Company to identify its customers and understand the purpose and intended nature of the business relationships.

The company conducts thorough and rigorous due diligence on each client to evaluate their status, identity, and suitability for the product/service in question.

The Customer Due Diligence (CDD) measures to be implemented include:

1. Identifying the client and verifying their identity using documents or information from a reliable and independent source.
2. Identifying the beneficial owner(s) and verifying their identity, understanding the ownership and control structure of the client, if applicable.
3. Assessing the purpose and intended nature of the business relationship (business profile).
4. Conducting ongoing monitoring of the business relationship and transactions to ensure consistency with the company's understanding of the client, business, risk profile, and source of funds.

GCB Suisse AG applies CDD measures in the following situations:

1. Before establishing a business relationship and providing any services to the customer.
2. Prior to conducting an occasional transaction.
3. In case of suspicion of Money Laundering or Terrorist Financing.

If GCB Suisse AG is unable to apply CDD measures to a client, it will:

1. Refrain from executing any transaction for the client.
2. Avoid establishing a business relationship with the client.
3. Terminate an existing business relationship with the client if necessary.

The Company should also consider submitting a suspicious activity report to the appropriate issuing institution or partner as applicable.

In addition to verifying the identity of the customer, GCB Suisse AG shall also gather information on the purpose and intended nature of the business relationship, including knowledge of the following elements:

1. Information on the projected turnover and scope of the business that the client intends to conduct with the company.
2. Details regarding the anticipated destination of payments.

3. Information about the business, its products, and services.
4. Details concerning the anticipated utilization of the services provided by GCB Suisse AG.
5. Expected amounts of monthly and yearly monetary transactions and the countries involved in the initiation or receipt of monetary transactions.

11. Identification of the Customer – natural person

The primary objective of Customer Identification is to ensure that the Company has a reasonable understanding of the identity of the customer/business.

The Company identifies the Customer who is a natural person and, when applicable, their representative, and maintains the following data on the Customer:

1. Valid Passport Copy or any other Government Issued ID document
2. Proof of Address
3. Email Address
4. Mobile Phone Number
5. Phone Interview (video requirement for annual purchases above CHF 5,000)

Other requirements:

1. Original documents must be presented to support the identity of each client, i.e. each individual or entity. The information must be stored in Golden Suisse central server databases.
2. Distance identification via the Internet is acceptable and authorised as part of the acceptance process.
3. All individuals identifying themselves must have their information verified and registered electronically via the Golden Suisse online application.

In addition to the aforementioned identification documents, GCB Suisse AG will accept other foreign country issued ID documents (e.g., foreign residence permit), provided they meet both of the following conditions:

1. The laws of the issuing country allow such document to be considered as a personal ID document for identification purposes; AND
2. The foreign ID document contains all of the following information: full name, personal code or date of birth, photo, citizenship (unless specifically not required

for such type of document), signature (unless specifically not required for such type of document).

Expired, damaged, or altered identity documents will not be accepted, and all four corners of the document must be visible. Each time any of these additional ID documents are utilized for customer identification purposes, GCB Suisse AG will ensure that it has examined the laws of the issuing country and confirmed that the document indeed holds the status of a "personal ID document" in that jurisdiction.

Normally, one of the following documents is required to verify proof of address:

1. Utility bill (telephone, television, gas, electricity, insurance, or water bill).
2. Bank statements.
3. Lease agreement.
4. Driving license displaying address (if it was not the document provided for identity verification).
5. Mortgage document (must be accompanied by proof of payment dated within the last 3 months; the mortgage document alone is insufficient, as it could indicate property sale).
6. Another valid government-issued ID showing the current address (provided it was not used for identity verification).
7. Electoral roll entry.
8. Salary statement; or
9. Credit card statement showing transactions.
10. Bank statement summary.
11. Health Insurance statement.
12. Extract from the Central Register of Residents (municipality of residence).

In order to comply with laws and regulations, mitigate risks, and prevent fraud, Golden Suisse implements AML KYC procedures for both prospective and existing clients. These procedures are translated into operational protocols, including process maps, work instructions, and forms utilized by the Golden Suisse team.

All clients are subject to screening through our KYC Spider System. For comprehensive information and step-by-step procedures, please refer to the KYC Spider Manual.

12. Enhanced Due Diligence

The Compliance Team of the Company is required to conduct inherent customer risk assessments before onboarding a customer. If a customer risk assessment results in High

Inherent Risk, Enhanced Due Diligence (EDD) measures must be implemented to mitigate identified risks.

EDD must be applied in the following circumstances:

1. When a Politically Exposed Person (PEP) is identified;
2. When financial crime-related adverse media is discovered;
3. When transactions are conducted to or from a high-risk third country;
4. When establishing a business relationship with a customer residing or incorporated in a high-risk third country.

Before onboarding a new high-risk customer, Senior Management must consult the MLRO. EDD measures should be applied for each high-risk case, in addition to regular Customer Due Diligence (CDD) measures.

The Compliance Team of the Company must consider the following situations as high risk:

1. Customer inherent risk assessment results in high risk;
2. The customer or a potential customer is a PEP, or a family member or known close associate of a PEP;
3. The client is involved in a business activity connected to a high-risk country;
4. The client resides, operates, or is incorporated in a high-risk country;
5. The customer is from a high-risk industry;
6. The customer conducts businesses or produces products that may present a higher risk of Money Laundering and Terrorist Financing (ML&TF);
7. Relevant Adverse Media is discovered;
8. In any case where a transaction is complex and unusually large, or there is an unusual pattern of transactions;
9. In any case where a transaction or transactions have no apparent economic or legal purpose;
10. Transactions performed to/from high-risk countries;
11. In the case of cross-border correspondent banking relationships with respondents domiciled outside the EU or domiciled in a state of the EEA, if an increased risk has been identified;
12. In case of an opaque ownership structure of a legal entity customer;

In any case where a customer provided false or stolen identification documents or any other information on establishing a relationship (a Unified Adverse Reporting (UAR) must be completed).

EDD measures must include:

1. Obtaining senior management approval to start or continue the business relationship;
2. Increased identification and verification of documents relating to the customer, directors, controllers, and/or beneficial owners;
3. Detailed inquiries to understand and validate the purpose and nature of the business relationship, including the client's source of wealth and/or source of funds, directors, controllers, and/or beneficial owners;
4. Obtaining additional information on the customer's occupation, volume of assets, information available through public databases;
5. Confirmation of expected activity to be transacted by the client;
6. Scrutiny of transactions utilizing automated/manual transaction monitoring systems;
7. Enhanced monitoring of the customer’s transactions;
8. Obtaining information on the reasons for intended or performed transactions;

Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

The following types of documents or information are a non-exhaustive list of types of EDD, which may be requested from the Client:

1. A certified company structure;
2. Annual audited accounts;
3. A credit reference (from a reputable credit reference agency);
4. Financial statements and banking references;
5. Business Plan;
6. Source of funds or source of wealth information in relation to a director, shareholder, the ultimate beneficial owner, or an end user;
7. Proof of employment of a shareholder, the ultimate beneficial owner, or an end user;
8. A copy of the most recent independent financial crime audit;
9. Proof of employment of a shareholder, the ultimate beneficial owner, or an end user.

As part of EDD, the following Source of Funds and Source of Wealth will be requested:

1. Identity proof and proof of address of all the directors and shareholders owning 10 % of shares or more;
2. Current Management Accounts;
3. Bank statements showing income not older than 3 months;

4. Documents confirming Source of Funds and Source of Wealth of the shareholders or/and beneficial owners;
5. Letter of secured or unsecured loan;
6. Wage slip or contract letter from employer;
7. Annual Income (confirmation from employer or tax filing);
8. Financial returns & audited accounts.

13. Sanction Screening

International sanctions are non-military measures used to impose constraints with the aim of promoting international peace and security. They serve as a legitimate foreign policy tool, wherein one or more countries impose penalties and restrictive measures against states, individuals, or entities that engage in actions such as human rights violations, contributing to territorial or religious conflicts, supporting terrorism, or violating fundamental norms recognized by the international community. GCB Suisse AG complies with and screens international sanctions against over 1000 databases in over 200 countries using KYC Spider, including but not limited to the following lists:

1. Swiss State Secretariat for Economic Affairs (SECO) sanctions lists;
2. The European Union's consolidated list of persons, groups, and entities;
3. The United Nations (UN) Security Council consolidated sanctions list;
4. The US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists;
5. The US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) list.
6. The UK HM Treasury (HMT)
7. Office of Financial Sanctions Implementation, "consolidated list of targets".

The screening will be conducted against the above-mentioned lists with the following frequency:

1. Prior to entering into a business relationship;
2. During the onboarding process;
3. Monthly, throughout the course of ongoing business relationships.
4. Immediately upon publication of any amendment to a screened sanctions or terrorism list (SECO, UN, EU);
5. Prior to processing any transaction where the counterparty has not been re-screened within the preceding 30 days.

Each potential match must undergo verification and investigation. A match will be considered false if it involves a different name, date of birth, gender, or place of incorporation (in the case of a legal entity client). The evaluation process of a match must be documented, and the Compliance member in charge must record the reasons for a particular decision made. A positive sanction hit must be reported to the MLRO immediately. Upon confirmation of a positive match against a screened sanctions or terrorism list, the Company must immediately freeze (Vermögenssperre) the relevant assets and business relationship in accordance with the applicable ordinance issued under the Embargo Act (EmbG, SR 946.231), and notify SECO without delay. The freeze takes effect immediately upon confirmation of the match; it is not deferred pending notification. Compliance must document, no less than monthly, confirmation that the KYC Spider sanctions list feed reflects the current SECO Consolidated Sanctions List version, with the confirmation date and list version recorded in the screening log. The company is prohibited from engaging in activities that are prohibited by international financial sanctions.
Where required, all potential and confirmed sanction matches encountered must be reported to the relevant issuing institution or authority.

14. Politically Exposed Person (PEP) screening

A politically exposed person (“PEP”) refers to any natural person who currently holds or has previously held a prominent public function, or an immediate family member of such an individual, or an individual known to be closely associated with them. Consistent with Art. 2a of the Swiss Anti-Money Laundering Act (GwG) and the VQF Regulations, the Company distinguishes between three categories of PEP, each subject to a different duration rule set out later in this Section 14: (i) Foreign PEP – a person holding or having held a prominent public function abroad; (ii) Domestic PEP – a person holding or having held a prominent public function in Switzerland at the national level; and (iii) PEP of an International Organization – a person holding or having held a leading role in an inter-governmental organization or an international sports federation.

Politically exposed persons specifically include:

1. Heads of State, Heads of Government, Ministers, Members of the European Commission, Deputy Ministers, and Secretaries of State.
2. Members of parliament and equivalent legislative bodies.
3. Members of the governing bodies of political parties.
4. Members of supreme courts, constitutional courts, or other high courts whose decisions typically have no further recourse.

5. Members of the governing bodies of audit institutions.
6. Members of the governing bodies of central banks.
7. Ambassadors, chargés d'affaires, and defense attachés.
8. Members of the administrative, management, and supervisory bodies of state-owned enterprises.
9. Directors, Deputy Directors, members of the governing body, or other leaders with comparable roles in intergovernmental international or European organizations.

Whether a function listed above constitutes a Foreign PEP, a Domestic PEP, or a PEP of an International Organization depends on the jurisdiction or organization in and for which it is held. This classification determines which duration rule under this Section 14 applies to the individual.

Close associate – a natural person who shares membership with a PEP in the same legal entity or non-legal entity body, or maintains another business relationship with the PEP, or is the sole Beneficial Owner of a legal entity or non-legal entity body established or operating de facto to acquire property or personal benefits for the PEP.

Close family members – the spouse, the person with whom the partnership is registered (cohabitant), parents, brothers, sisters, children, children’s spouses, and children’s cohabitants.

Known Close Associate – means a known close associate of a PEP as being either an individual known to have joint beneficial ownership of a legal entity, legal arrangement or any other close business relationship with a PEP. Also, an individual who has sole beneficial ownership of a legal entity, or a legal arrangement, which is known to have been set up for the benefit of a PEP.

For the purposes of the duration rule below, a close family member or known close associate of a PEP is classified in the same category – Foreign, Domestic, or International Organization – as the PEP to whom they are related or associated. The duration of their PEP-adjacent classification accordingly tracks that of the underlying PEP and does not run independently of it.

The duration of PEP status differs strictly by category and does not follow a single rule for all PEPs. A Domestic PEP ceases to be classified as a PEP under this Policy 18 months after the individual ceases to exercise the qualifying public function, in accordance with Art. 2a GwG; from that point, the Company's ordinary risk-based due diligence applies in place of PEP-specific Enhanced Due Diligence. A Foreign PEP and a PEP of an International Organization – together with their close family members and known close associates – benefit from no such time-based cessation: their classification remains in

effect indefinitely, regardless of how many years have elapsed since the individual left the qualifying function, and regardless of any other change in personal circumstances. No declassification of a Foreign PEP, a PEP of an International Organization, or their close family members or known close associates is permitted on the basis of elapsed time alone.

Any declassification of a Domestic PEP under the 18-month rule above must be approved by the MLRO and documented in the client file, recording the date the qualifying function ceased and confirming that no additional risk indicators are present; risk-sensitive ongoing monitoring must continue until the MLRO confirms that the risks commonly associated with PEP status no longer apply. Because Foreign PEPs and PEPs of International Organizations – and their close family members and known close associates – cannot be declassified on the basis of time elapsed, the Company instead applies a risk-based recalibration: where such a relationship has been maintained over a significant period without adverse findings, the MLRO may approve, in writing, a reduced-intensity Enhanced Due Diligence regime appropriate to the assessed residual risk (for example, an extended KYC refresh interval or an adjusted transaction-monitoring threshold). Any such recalibration must be dated, reviewed at least annually, and immediately revisited upon any change in circumstances or adverse information; it reduces the intensity of monitoring applied but does not remove the PEP classification, the EDD requirement, or the Company's reporting obligations.

Because high-profile political figures can pose a higher risk of money laundering, Enhanced Due Diligence (“EDD”) must be applied to all PEPs, in every category, for as long as their PEP classification remains in effect – including where a reduced-intensity regime has been approved under the recalibration mechanism described above. Application of EDD enables the Company to understand the source of wealth and source of funds relating to the PEP and to build a transactional and customer profile to monitor transactions and PEP customer behavior.

The screening will be performed by third party provider KYC Spider, against the details obtained in the identification documents which were collected during the customer due diligence process. Re-screening must occur each month. Re-screening must occur each time relevant Sanctions or PEP lists change.

Every potential match must be verified and investigated. A match can be considered as false in case it is based on a different name, a different date of birth, a different gender, a different place of incorporation (in case of a legal entity client).

15. Adverse Media Screening and Special Interest Persons (SIP) Screening

As part of Due Diligence verifications, the Company must conduct adverse media searches. The Company must understand the reputation of its clients and must be aware whether they were previously investigated for any criminal offense committed or if any penalties were applied to them.

Every potential match must be verified and investigated. In case the relevant member of the Compliance Team will not be able to discount a match, it must be referred to the MLRO of the Company who will decide what further action is required.

All financial crime-related adverse media matches should be escalated internally and, if required, reported to the relevant authority.

16. Transaction Monitoring

GCB Suisse AG will conduct ongoing monitoring of its customer relationships.

Throughout the duration of a customer's account relationship, the company will observe the activity within the account and scrutinize transactions to ensure they align with the company's understanding of the customer, their business, and risk profile, as well as the source of funds when applicable.

The company will give particular attention to any complex, unusually large, or suspicious transaction patterns that lack an apparent economic or legal purpose.

For ongoing monitoring purposes, GCB Suisse AG has implemented adequate systems and processes tailored to the size and complexity of the company. This includes monitoring the account relationship with the customer, ensuring compliance with the company's requirements, and detecting and reporting suspicious or unusual transaction patterns.

Whenever possible, the company will inquire about the background and purpose of such transactions and document its findings for potential disclosure to relevant authorities if necessary. If unusual patterns are identified, enhanced due diligence will be conducted, which may involve establishing the source and destination of funds, obtaining more information about the client's business, and monitoring the business relationship and subsequent transactions more closely.

Any suspicious activity will be reported to the MLRO for further investigation or reporting to the relevant authorities.

17. Ongoing Monitoring and Client Reviews

GCB Suisse AG will adopt a risk-based approach to continuously monitor its clients for signs of money laundering, with a focus on transaction monitoring and client reviews. The company will apply varying levels of monitoring based on the risk rating assigned to each client.

As part of ongoing monitoring, the company will ensure that customer documents, data, and information are updated at appropriate intervals.

The Company's Compliance Team must conduct periodic reviews of its customers, with the frequency of these reviews depending on the risk level posed by each client. The specific time frames for reviewing the accuracy of customer data are as follows:

1. **Low-Risk Customers** – reviewed once every three years. This interval is based on the low risk of money laundering determined by the Customer Risk Assessment (CRA) conducted by the company.

2. **Moderate-Risk Customers** – reviewed once every two years. If the CRA results in a medium risk of money laundering, the review of customer data accuracy must be conducted within a two-year period.

3. **High-Risk Customers** – reviewed annually. For customers identified as posing a high risk based on the CRA results, data updates must be performed on an annual basis.

The customer risk assessments conducted on the existing customer base must also be reviewed to capture any changes that may have occurred.

Whenever a triggering event occurs, such as anomalies detected during continuous monitoring, identification of a Politically Exposed Person (PEP), discovery of financial crime-related adverse media, or a previously unidentified match with sanctions, the customer must undergo a thorough review.

In the event of changes in a customer's circumstances, such as changes in corporate structure, ownership and control, customer base, required products, jurisdictional scope of operations, transaction types, etc., a reassessment must be conducted.

Enhanced ongoing monitoring must apply to all clients that were assigned a high risk. It should be applied to all PEP relationships.

18. Suspicious Activity Reporting

The Company defines suspicious activity as any activity that deviates from normal or usual practice. Furthermore, the Company acknowledges that its business activities may potentially involve suspicious activity.

The purpose of reporting suspicious activity is to report any known or suspected violations of the law or suspicious activities observed by the Company's internal teams. It is crucial that all staff members are able to identify potential signs of fraud, money laundering, and terrorist financing.

The following behaviors should be considered suspicious:

1. The customer fails to provide the required data and is unresponsive.
2. The customer submits incomplete or incorrect data.
3. The customer or its representative avoids providing the necessary data to establish its identity, conceals the identity of the beneficial owner, or avoids providing information necessary to establish the identity of the beneficial owner.
4. It is not possible to determine whether the customer operates on its own behalf or is controlled by someone else.
5. It is not possible to understand the ownership and control structure and the nature of the customer's business (in the case of a legal entity client).
6. It is not possible to obtain information about the purpose and intended nature of the customer’s business relationship.
7. It is not possible to verify the identity of the customer and the beneficial owner according to documents, data, or information obtained from a reliable and independent source.
8. An address provided by the customer to identify an individual's residency or company's operational placement appears vague, unusual, or cannot be found on Google Maps.

All employees of the Company must report any unusual and/or suspicious activity to the MLRO using an internal Unusual Activity Report (UAR). The report should include the date of completion, the employee's name and department, details of the suspicion (related to money laundering, terrorist financing, or other concerns), information about the subject of the report, and any other relevant details that the employee deems necessary.

If an individual is suspected, the report must include the individual's full name, date of birth, gender, identity number, country where the identity number was issued, occupation, address, contact details. The same details for any other associated parties suspected must also be included in the UAR report.

The reasons for suspicion must be disclosed in detail, along with all relevant details about the suspicious transactions and the suspicious customer's behavior. Information about due diligence performed must also be included in the report.

After an Unusual Activity Report in relation to a particular customer has been shared with the MLRO, the onboarding of that client or a particular transaction conducted by that client must be halted.

The MLRO must analyze the UAR report and determine whether the suspicions are justified. If the suspicion is validated, the MLRO must proceed with submitting a suspicious activity report to the relevant authority. The results and conclusions related to the investigations of the customer's activity and transactions must be documented.

In case of externally managed programs, unusual activity reports must be submitted to the relevant issuing institution or partner in line with applicable agreements.

19. The Exit of a Business Relationship

The company may decide to terminate a business relationship under the following circumstances:

1. If the customer refuses to provide additional information upon request within specified time limits.
2. If, during ongoing due diligence, the company identifies a significant change in the customer's ML/TF risk that cannot be effectively mitigated.
3. If the company discovers information indicating that the customer is using the product/service for ML/TF or is involved in criminal or fraudulent activity (a UAR must be completed).
4. If the customer's name or that of its associated party appears on sanctions lists.
5. If the customer attempts to use forged documents or provides false information
6. If the customer fails to provide identity confirmation information or deliberately withholds information required to identify beneficial owners and/or directors.
7. If it is unclear whether the customer is acting on their own behalf or under someone else's control.

8. If the customer's ownership structure cannot be determined.

The aforementioned situations must be assessed, and the MLRO must be notified immediately.

The recommendation for terminating a business relationship is made by the MLRO. An internal register must be maintained containing the names of clients with whom a business relationship has been terminated.

20. Training

GCB Suisse AG is required to provide suitable AML/CTF preventive controls training to ensure that employees are well-versed in identifying risks and suspicious activities and transactions that may arise from the nature of the Company's business.

GCB Suisse AG will ensure that all relevant employees are knowledgeable about relevant legislative and regulatory requirements. Employees will receive training on AML laws and internal policies and procedures, supervised by the MLRO.

The MLRO must ensure that each new employee undergoes appropriate money laundering prevention awareness and training upon starting their job at GCB Suisse AG or within 30 days of joining (induction training). Subsequently, refresher training must be conducted at least once a year thereafter or as needed (specific training).

The company should maintain a register of conducted training, including the pass level, date, and the name of each employee who attended the training session.

21. Employee Awareness

It is The Company’s policy to ensure that all employees are aware and kept up to date with money laundering developments. This Policy serves as the basis for awareness within the Company. It will be supplemented with additional material as and when necessary. It is the responsibility of the MLRO to ensure that all employees of the Company are kept up to date with changes to both regulatory and Best Business Practice regimes.

At the start of their employment every employee must read this Policy.

22. Record Keeping

All retention and handling of personal data must adhere to the Company's Data Protection Policy and local requirements.

The Company must retain the following for a period of at least five years following the termination of the customer relationship:

1. Customer Due Diligence (CDD) information, including copies of documents verifying the identity of the client, as well as other data collected during the due diligence process (e.g., invoices, contracts, Source of Funds/Source of Wealth documents).
2. Customer Risk Assessments (CRAs) conducted, with calculations stored in the client's relevant folder.
3. Records of transactions conducted, including relevant documents and data confirming monetary transactions.
4. Details of internal and external suspicious activity reports.
5. Records of sanctions, embargo, and terrorism list screening, including the list version/date used, matches identified, verification outcome and rationale, and any escalation or SECO notification (retained for no less than five years).
6. Records of training conducted for company staff.

All internal compliance records will be stored electronically for a minimum of five years. Customer records will be retained for at least five years from the end of the business relationship or occasional transaction. The MLRO is responsible for ensuring that customer records are appropriately disposed of in accordance with data security best practices.

The processing of registered customer information is restricted to fulfilling the company's contractual obligations towards the respective customer or complying with the rules and obligations outlined in the Company's Policies. Any employee with access to registered personal information is bound by a duty of confidentiality. Documentation folders will be securely stored with strict access controls.

ANNEX

UNUSUAL ACTIVITY REPORT (Template)

STRICTLY PRIVATE, CONFIDENTIAL AND LEGALLY PRIVILEGED

Date:	DD/MM/YYYY
To:	MLRO / Relevant Issuing Institution (To be directed to the appropriate authority as defined under applicable procedures v2.)
From:	

NOTES: -

(1) If the information in the template is in *italics*, it is likely what will go in the form, or it is the choices that are on the NCA input form.
(2) "**Main Subject**": - There should only be one "Main Subject". If the "Main Subject" is a Company use the "Main Subject (Company)" template. If the "Main Subject" is and Individual use the "Subject One ("Individual") but entitle it "Main Subject (Individual)".
(3) "**Associated Subject**": - If there are multiple Company" suspects, provide the information for any company/entity that we have information on, using the "Main Subject (Company)" format. There can be multiple ones.
(4) "Associated Subject": - If the Associated Suspects are individuals use the "Associated Subject (Individual)" format to provide any individual associated subjects (there can be multiple).

General Details		
Disclosure type:	This Report concerns unusual activity relating to potential:	
	☐	Money Laundering
	☐	Terrorist Financing
	☐	Another
	If you have chosen "Another", please describe briefly why:	

New or existing disclosure ID:	☐	Unusual activity relates to a previous report you have or you know has been provided to the MLRO
	If selected, please provide the details below:	

Main Subject (Company)	
Legal entity Name:	
Trading Name:	
Legal entity Registration Number:	
Formation Date	*DD/MM/YYYY*
Business type	
VAT number:	"*VAT Number" or "N/A*"
Country of registration:	
Address:	Building Number: - Street: - City: - Country: - Post Code: -
Address type:	"*Registered Address" or "Place of Business*" [If there are more than one addresses, and it is possible to list them, do so.]
Contact details:	Email Address(s): - Business Telephone Number(s): - Skype Name: - Other contact Information and description: -
Details of Beneficial Ownership:	
Other Relevant Information:	*[Any other relevant information, such as a change of Director, change of company name, or anything like that.]*

Associated Suspect One (Individual)	
Individual names:	Last Name: - First Name: - Other Names: -
Date of birth:	DD/MM/YYYY
Gender:	Female / Male
Occupation:	[*If known*]
Identity number(s)	*[If more than one list all we have.]*
Identity type(s)	*[e.g. "Passport Number"; "National Identity Number"; Social Security Number}*
Country of Identity Number(s):	
Account number:	
Address:	Building Number: - Street: - City: - Country: - Post Code: -
Address type:	*[e.g. "Residence address"; "Domicile"]*
Contact details:	Email Address(s): - Business Telephone Number(s): - Skype Name: - Other contact Information and description: -

ADD FURTHER ASSOCIATED SUSPECTS IF NECESSARY

Reasons for suspicion
Background **Related Programme Manager** Who is the PM / What is the Product? **Background of Cardholder & Suspicious Transactions** Details (other than KYC / KYB) of the cardholder or account holder use of the product (i.e. when was the account opened, relevant loading, relevant spending, relevant communication with the cardholder or account holder). **Enhanced Due Diligence** What enhanced due diligence was carried out or attempted and what was the response (if any)? **Relevant transaction(s)** Detail all transactions relevant to the suspicion or knowledge of ML / TF in chronological order. **Reason for Suspicion/Knowledge** Full reasons for suspicion or knowledge of ML / TF required. **Consent** Is there a balance on the card which requires us to hold it prior to any police investigation or recall request or are we required return it to the Suspect or bank making a recall request? If so, what is the balance? If zero balance, state "*0 – No consent required*".