Anti-Money Laundering and Compliance Policy

As prepared by **CFS-Zipp Limited** on May 2016

CFS-ZIPP LIMITED
790 UXBRIDGE ROAD
HAYES
MIDDLESEX
ENGLAND
UB4 0RS, UNITED KINGDOM

Table of Contents

Our AML Policy

What is this guide?

This document is a general guide defining Anti-Money Laundering (AML), Counter Terrorist Finance (CTF), Counter Fraud Procedures, regulations, Risk-Based approach and gives some examples of what can be deemed to be money laundering. It further gives you an idea of what CFS-Zipp does and how we protect ourselves and our customers, through thorough due diligence, from Money Laundering and Terrorist Financing threats.

Why do I need to read this guide?

This guide is for CFS-Zipp Limited (CFS-Zipp) employees, senior management, foreign correspondents, contractors and third parties with whom CFS-ZIPP may contract with (Agents, UK MSB customers). The guide offers advice about ways in which you can fulfil your legal obligations.
The law does not specify the measures you must take to comply with its requirements, but rather sets guidelines within which organisations must operate. This information guide therefore offers advice on the ways that you can perform these duties effectively.

How will this guide help me?

Very simply, it will help you follow the law!

What is Money Laundering?

Before starting at CFS-Zipp, it is important you have a basic understanding on what Money Laundering is, why it is important to prevent it, and how we go about doing that on a daily basis.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

- **Placement:** Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions.
- **Layering:** Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.
- **Integration:** Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

It also covers money, however acquired, which is used to fund terrorism. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

What is criminal property?

Criminal property is the proceeds of criminal conduct. This includes any type of conduct, wherever it takes place, which would constitute a criminal offence if committed in the UK. It includes drug trafficking, terrorist activity, tax evasion, corruption, fraud, forgery, theft, counterfeiting, black mail and extortion. It also includes any other offence that is committed for profit.

The Money Laundering Regulations (MLR)

The Money Laundering Regulations 2007 (HMRC) require relevant businesses to have:

- Policies and procedures to prevent them from being used by money launderers.
- Employees trained in these procedures and in anti-money laundering law.

- Checks and controls to ensure that the policies and procedures are working.
- Have internal and external measures in place for the disclosure procedures for suspicious transactions.

Regulation 20 of The Money Laundering Regulations 2007 sets out the requirement for relevant businesses to establish and maintain appropriate and risk-sensitive policies and procedures relating to:

- Customer due diligence
- Reporting
- Record keeping
- Internal control
- Risk assessment and management (Risk Based Approach)
- The monitoring and management of compliance, and
- The internal communication of such policies and procedures, in order to prevent activities related to money laundering and terrorist financing.

These policies and procedures must:

- Identify and scrutinise
    - Complex or unusually large transactions
    - Unusual patterns of transactions which have no apparent economic or visible lawful purpose
    - Any other activity which could be considered to be related to money laundering or terrorist financing
- Specify the additional measures that will be taken to prevent the use of products and transactions that favour anonymity for money laundering or terrorist financing
- Determine whether a customer is a politically exposed person (see Annex 5 for definition and further guidance)
- Nominate an individual in the organisation to receive disclosures under Part 7 of PoCA 2002 and Part 3 of the TA 2000.
- Ensure employees report suspicious activity to the Nominated Officer, and
- Ensure the Nominated Officer considers such internal reports in the light of available information and determines whether they give rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.
- Financial institutions (which include bureau de change, money transmitters and cheque cashers) must, additionally:
    - Establish and maintain systems which enable a full and rapid response to enquiries from law enforcement agencies, and

- Communicate the policies and procedures to branches and subsidiary undertakings which are located outside the UK.

The main principles encompassed by The Money Laundering Regulations 2007 can be described as *Risk Based Approach (RBA).* RBA requires a number of steps to be taken to determine the most cost-effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the business. The steps are to:

- Identify the money laundering and terrorist financing risks that are relevant to the business
- Assess the risks presented by the particular
  - Customers – types and behavior
  - Products and services
  - Delivery channels, for example, cash over the counter, electronic, wire transfer or cheque
  - Geographical areas of operation, for example, location of business premises, source or destination of customers' funds
- Design and implement controls to manage and mitigate these assessed risks
- Monitor and improve the effective operation of these controls and
- Record appropriately what has been done, and why

Please see Annex: 1 for detailed explanation of Risk Based Approach.

Where can I find more information?

Check out the following website that contain the details of different issues discussed in this document and is likely to be useful during your time with us:

1. Joint Money Laundering Steering Group: www.jmlsg.org
2. Financial Conduct Authority (FCA) website: www.fca.org.uk
3. HM Revenue & Customs (HMRC): www.hmrc.gov.uk/ which has detailed information on anti-money laundering regulations.
4. Office of Foreign Assets Control (OFAC): www.treasury.gov/ofac
5. HM Treasury: www.hm-treasury.gov.uk
6. Financial Action Task Force ("FATF"): www.fatf-gafi.org
7. FinCEN advisory list: www.fincen.gov

Terms and Definitions

These are terms you should be familiar with.

Terms/Acronyms	Definition
Nominated Officer	A Nominated Officer (also known as the MLR officer) is the focal point within the company for the oversight of all activity related to anti-financial crime issues.
Supporting Officer	A person or persons nominated to act on behalf of the Nominated Officer.
AML	Anti-Money Laundering
KYB	Know Your Business
KYC	Know Your Customer
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
MLR	Money Laundering Regulations
NCIS	National Crime Intelligence Service
PEP	Politically Exposed Persons
SAR	Suspicious Activity Report
NCA	National Crime Agency

Our Products and Services

To give you a small overview, CFS-Zipp focuses its business in 4 different areas: E-Wallets, E-Vouchers, Individual Merchant Services and Technology Outsourcing. To manage our risk effectively, we conduct business online via online transactions and do not deal in any cash. Moreover, any Agent of CFS-Zipp is fully vetted prior to on-boarding and are integrated into our compliance procedures and protocols.

E-Wallets

CFS-Zipp E-Wallet accounts can be set up by businesses looking to make payments to registered individuals or suppliers. This is done through our registered Agents of CFS-Zipp and through our very own platform. Both the business accounts and the individual accounts are subject to KYC checks prior to registration on their designated platform and they may be subject to occasional compliance checks on certain transactions. Details on how to conduct due diligence on Individual and Business Accounts can be found in this document. We are planning to introduce virtual and physical cards in connection to the E-Wallets as well.

E-Vouchers

CFS-Zipp can issue E-Vouchers and this is something we are exploring. E-voucher issuing comes with its own set of compliance requirements to ensure that they are not being used to redeem on websites dealing in unregulated/unlicensed gaming/gambling, adult sites, online dating, pharmaceuticals/medicines, arms/weaponry, and for redemption in unregulated areas. This has also been explored in this document.

Merchant Services

CFS-Zipp provides merchant and corporate services for different businesses. This can include invoice payments, payments to retailers and suppliers, payroll processing etc. These is also built into the E-Wallet system.

Technology Outsourcing

CFS-Zipp Technologies is a sister company and Agent of CFS-Zipp that is working on the development and outsourcing of a banking and compliance software for other businesses. Compliance here is limited to vetting the businesses leasing our software and is generally low-risk.

Now that you have an understanding of what we do, the rest of the document will give you an overview of compliance procedures to be applied to the above services.

Internal Controls and Communication

Money Laundering Regulations 2007 requires businesses to have appropriate systems of internal control and communication in order to prevent activities related to money laundering and terrorist financing. In simple terms this means that businesses must ensure that management controls are put in place that will alert the relevant people in the business to the possibility that criminals may be attempting to use the business to launder money or fund terrorism, so as to enable them to take appropriate action to prevent or report it.

Systems of internal control and communication must be capable of identifying unusual or suspicious transactions or customer activity, of identifying transactions and business relationships specified in a direction issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act, and enabling prompt reporting of the details to the Nominated Officer/Money Laundering Reporting Officer (MLRO) (see Section 2 page 10 of this guide) or to the owner of the business, who is responsible for making a disclosure to National Crime Agency (NCA) under the terms of the PoCA 2002 or the TA 2000.

The nature and extent of systems and controls that the business needs to put in place will depend on a variety of factors, including the:

- Degree of risk associated with each area of its operation
- Nature, scale and complexity of the business
- Type of products, customers, and activities involved
- Diversity of operations, including geographical diversity
- Volume and size of transactions, and
- Distribution channels.

CFS-Zipp periodically carries out and records checks to ensure our systems are working in practice. Where systems are found not to meet with the needs of the business or at worst they are not working in practice, we will record the action we are going to take to rectify the problem. We will also look at ways to ensure that we review the systems and process of the organisation to ensure that they are fit for purpose.

The Money Laundering Reporting Officer (Nominated Officer)

A *Nominated Officer* is the person within an organisation who is responsible for overseeing all activity related to anti-money laundering matters. Please familiarize yourself with the below personnel as you should be working closely with them.

CFS-Zipp's **Nominated Officer** is Dr. Srinivas Venkatesh.
In the absence of the Nominated Officer, Supporting Nominated Officers will take his/her place.
CFS-Zipp's **Supporting Nominated Officer** is Mr. Ganesh Sankraran
CFS-Zipp's **Compliance Officer** is Ms. Karthika Harish Venkatesh

The Nominated Officer's responsibilities include:

- Receiving disclosures from employees (also known as Suspicious Activity Report-SAR's).
- Deciding if disclosures should be passed on to the National Crime Agency (NCA).
- Reviewing all new laws and deciding how they impact on the operational process of the company
- Preparing a written procedures manual and making it available to all staff and other stakeholders
- Making sure appropriate due diligence is carried out on customers and business partners
- Receiving internal Suspicious Activity Reports (SARs) from staff
- Deciding which internal SAR's need to be reported on to NCA
- Recording all decisions relating to SARs appropriately
- Ensuring staff receive anti-financial crime training when they join and that the receive regular refresher training
- Monitoring business relationships and recording reviews and decisions taken
- Making decisions about continuing or terminating trading activity with particular customers
- Making sure that all business records are kept for at least five years from the date of the last customer transaction as per FCA regulations

The nominated officer is a person who has sufficient authority and autonomy in order to make the decisions required above. The Supporting Nominated Officer shall replace the Nominated Officer when he/she is unavailable.

Staff Training and Reporting

Training will be given to all new employees before they start work and will be repeated every 12 months as a refresher. We will also carry out training where there has been a substantial change in the law.

All staff will be fully trained using the CFS-Zipp AML Presentation and this AML Policy. Both are regularly updated and checked by professional compliance consultants.

All awareness training activity shall be recorded and filed by the Nominated Officer. The Nominated Officer will provide a monthly review of business activity with the staff, to ensure all procedures and processes have been adhered to with all customer registrations and ensuring that business transactions have been completed correctly.

Role of the Employee

If you are in the "regulated sector" and have "reasonable grounds for knowing or suspecting money laundering", you must report this to your Nominated Officer "as soon as is practicable". By failing to report a suspicion an employee may be committing an offence (see below).

Under what circumstances could I commit an Offence?

You can commit an offence if, when your suspicions are aroused, you:

- Willfully turn a blind eye to the obvious,
- Fail to adequately ascertain the facts, or
- Fail to make adequate enquiries to assure yourself of the legitimacy of the transaction.

What do you mean by 'Suspicion'?

Suspicion can occur in circumstances that suggest to a reasonable individual that a person might be laundering money. Suspicion must be more than a mere hunch. Any activity that does not fit with the normal course of business, or is not normal for a particular client should be regarded as suspicious.

What do you mean by a Transaction?

A transaction is anything you carry out by way of business.
Suspicion indicators for **new customers** can include:

- Checking their identity is proving difficult,
- The customer is reluctant to provide details of his/her identity,
- There is no genuine reason for the customer to use the services of a merchant, and

- Where transactions involve international transfers or foreign currency, the explanation for the business and the amount involved is unreasonable.

Suspicion indicators for **regular and established customers** include the:

- Transaction is different from the normal business of the customer,
- Size and frequency of the transaction is not consistent with the normal activities of the customer, and
- Pattern of transactions has changed since the business relationship was established.

How do I report my suspicion to the Nominated Officer?

You should report the grounds for your suspicion to your Nominated Officer in line with your employer's internal procedures. You should include full details of the identification you have and any other customer information you have.

When should I report my knowledge or suspicion to the Nominated Officer?

You must do this as soon as is practicable after you have reasonable grounds for suspicion. If you do not do this you may be committing an offence.

What does "as soon as is practicable" mean?

This means as soon as you reasonably can. Internal reporting lines to your Nominated Officer should be short in order to avoid delay.

What if I become suspicious before I complete the transaction?

You should make an internal report before the transaction is completed and wait for consent from your Nominated Officer before you complete the transaction.

What should I say to delay the transaction without "tipping off" the customer?

Give the customer an excuse that fits the circumstances. In difficult cases speak to your Nominated Officer or manager.

If I think delaying the transaction would "tip-off" the customer, can I go ahead?

Ask your Nominated Officer. They may let you proceed with the transaction, but this should not be done routinely. The reason why you think delaying the transaction would "tip off" the customer must be included in your report.

What should I do if the customer asks for his money back before I get consent from the Nominated Officer?

Seek advice from the Nominated Officer urgently.

What if I become suspicious after the transaction has taken place?

Make an internal report to your Nominated Officer as soon as you can.

What if I refuse the business?

If you refuse the business because you are suspicious, you must still make a disclosure to the Nominated Officer. You must obtain evidence and keep records of the customer's identification as soon as you become suspicious.

Identifying the Customer

You will need to confirm that your customer/client is who they say they are by completing relevant 'Know Your Customer' (KYC) checks.

Hosts of CFS-Zipp's platform or those Hosts not managed by CFS-Zipp, if issuing e-money through CFS-Zipp, will be responsible for collecting, ratifying and storing KYC information for their customers/client. CFS-Zipp maintains full visibility on all transactions on a day-to-day basis and signs off on all KYC checks.

All Host managers must ensure that they adhere to the KYC & AML procedures documented in this CFS-ZIPP Anti-Money Laundering (AML) Guide.

'KYC' - What does 'know your customer' mean?

KYC means obtaining information about a customer over and above the required ID.

The purpose of this is to reduce the risk of your business being used for money laundering. Although there is no legal requirement for you to do this, asking your customers questions such as their reason for establishing business with you, the source of their funds and the anticipated level and nature of the activity to be undertaken can increase the likelihood that you will detect suspicious activity.

Multiple online directories of individual and business information are used to check all customer/client ID details before a full Individual or Business e-account is activated.

For Business clients we also check their details against the UK registered companies database held by Companies House; the United Kingdom Registrar of Companies, it is an Executive Agency of the United Kingdom Government Department for Business, Innovation and Skills (BIS).

The following "Know Your Customer" procedures will be helpful in identifying prospective customers who may present money-laundering risks. While not all of these procedures are necessary in every instance, they should be considered and documented as part of standard account opening procedures.

In all cases, prior to taking on a new customer or engaging in a transaction with a customer with whom you do not have well-established relationship, you need to complete sufficient due diligence to have confidence in the integrity of the customers and the lawfulness of the proposed transaction.

1. Make reasonable efforts to determine the true identity of all customers and the legal and beneficial ownership of all accounts.
2. Determine the customer's citizenship, home and business addresses, occupation or type of business. Where appropriate, obtain supporting documentation.
3. Inquire whether the customer will have the sole interest in the account or whether there will be other persons who will have access to it. Verify the identity of all such persons and engage in any necessary due diligence regarding such other persons.
4. If the customer is not an individual;
    a. Determine the legal status (e.g., corporation, partnership or other form of entity).
    b. Determine whether the customer is regulated, either in the UK or a foreign country.
    c. Determine all principal persons of the customer, such as officers and directors, or persons who have a substantial beneficial interest (i.e. own more than 20% share in the company).
    d. Obtain copies of all relevant organisational documents.
5. Identify the source of the customer's funds.
6. Screen the account for;
    a. Matches under the OFAC list.
    b. HM Treasury list
    c. Account holders from countries listed on the Financial Action Task Force ("FATF") NCCT list found at http://www1.oecd.org/fatf/NCCT_en.htm or the FinCEN advisory list at http://www.occ.treas.gov/Adv1st02.htm.
7. Where appropriate, obtain information regarding the frequency with which the customer expects to transfer funds to or from the account, i.e. monthly, quarterly, or the nature of any third-party payments to or from the account.
8. Where appropriate, obtain and contact reputable references, such as professionals and other members of the financial industry, banks, securities companies, etc.
9. Government Officials and Foreign Bank Accounts;

Special procedures apply for accounts for the benefit of senior government and political figures, particularly from certain countries, and for accounts opened by or through foreign banks. Inasmuch as this is not a regular part of the Company's business, you must consult the Compliance Officer before opening any account of this type.

10. Accounts through an Intermediary;

Where accounts come through an intermediary, the Agent must either perform due diligence with respect to the account or satisfy itself that the intermediary has performed the type of due diligence with respect to the account that would satisfy the Agent's "Know Your Customer" policy.

a. The scope of this due diligence will vary depending upon the Agents historical relationship with the intermediary, whether the intermediary is itself a regulated entity and the jurisdiction in which the intermediary is located. The Compliance Officer should be consulted as to the type of due diligence necessary for a specific intermediary.
b. At a minimum, due diligence of an intermediary should include a review of the intermediary's anti-money laundering procedures. Where appropriate, representations from the intermediary as to its compliance with its procedures may be obtained.
c. Generally speaking, except for intermediaries who are regulated in an appropriate jurisdiction or are well-known by the Agent to have proper anti-money laundering procedures in place, you should perform reference checks through published sources and others.

11. Counterparties;

The same rules set out in item 10 above also apply to transactions with counterparties on behalf of our customers. For this purpose counterparties include private transaction counterparties and banks and other dealers, agents and intermediaries. While a relatively low level of due diligence will be required for counterparties who are regulated within a country known to have appropriate and well-enforced anti-money laundering regulations, other counterparties will require the same level of due diligence as clients.

Notes:

If it is proving difficult to identify a new customer, be on guard and refer the case to the Nominated Officer for guidance.

All companies registering will need their company director to sign a Company Members form to say that they are either the main user for the e-account or that they consent to an additional user to use the e-account on the company's behalf, that they have read the Terms and Conditions for using CFS-Zipp e-account and they accept liability for all the transactions undertaken by other users who have the authority to use and operate their CFS-Zipp e-account.

Customers have access to their e-account through our secure website. For general guidance, ensure that customers DO NOT disclose their user name and password for other people to use. This is a breach of our security requirements and should be reported to our Nominated Officer, if it should occur. We advise Business e-account holders that if they wish to allow other staff members to use the facility for their business needs, then those staff members need to be registered and verified separately before we can link the two e-accounts together.

Account Opening Process

Individual e-Account

If a customer submits an Individual e-account registration form online (currently individual accounts can only be done through a merchant's E-Wallet), they will automatically have access to a Limited e-account. Before we can upgrade their e-account to a full Individual e-account (wherein they can actually load the account and start transacting) CFS-Zipp Customer Services will need to verify some details and collect all the necessary documents.

All individual account holders as such would have to provide a certified photo ID and proof of residence (e.g. Utility bill) for their accounts to be fully activated and operational. Limited e-account holders should send a copy of their certified photo ID, i.e. International Passport, UK Driving License, UK Residence Permit, Visa Work Permit or other Verification ID and a copy of their proof of residence to CFS-Zipp.

These can be scanned and emailed to CFS-Zipp Compliance at: compliance@cfszipp.com

Successful applicants will be notified via email that their *Limited* e-account has been upgraded to a *Full Individual* e-account.

Please note; If necessary, additional information may be requested by CFS-Zipp on the details regarding the nature of certain transactions.

All hard & soft copies of documentation from individual customers will be retained for a minimum of five years. All verified documents will be reviewed annually to ensure that they are: a) still relevant to the activity being carried out by the customer and b) are still valid (i.e. the ID documents provided have not expired).

Business e-Account

The Business e-account has been designed for businesses wishing to set up an e-wallet or that require merchant services. A Limited Business e-account will be opened automatically after businesses have submitted their completed registration form online. Within 48 hours of submitting their registration form they will be contacted by telephone or email by a member

of our CFS-Zipp team who will provide further information on what details need to be submitted before the Business e-account can be upgraded to a Full Business e-account. It is only then that the account can be operational.

Details should include:

- A completed CFS-Zipp Business Account Application Form with signed T&Cs,
- Incorporation documents; certificate, Memorandum of Understanding & Articles of Association, company utility bill (proof of address registered against CFS-Zipp e-account),
- Details of ownership (those persons or entities which hold 20% or more shares), directors and personnel who will be operating your e-account on behalf of the business, including copy of passport and utility bill,
- Information regarding the nature of their business; including the amounts of money involved and the expected frequency of transactions. During this stage, the reason for using CFS-Zipp services, the nature and level of the activity to be undertaken and the origin and destination of the funds should be clarified and noted.
- Any business related certification
- Any other relevant information regarding the business operations relating to use of our interface/platform,
- If necessary additional information may be requested by CFS-Zipp on the details regarding the nature of certain transactions.

If it is deemed necessary please ask for all or selected Business KYC information to be certified as a true copy of the original by a solicitor.

This information should be emailed or sent to CFS-Zipp via post.

Successful applicants will be upgraded to a Full Business e-account and notified of this via email.

Please note; Business e-account limits can be negotiated and tailored to a business's operational requirements.

All hard & soft copies of documentation from business clients will be retained for a minimum of five years. All verified documents should be reviewed annually to ensure that they are: a) still relevant to the activity being carried out by the business customer and b) are still valid (i.e. the company registered details and key company personnel details are still the same).

Common Questions on KYC

What is a business relationship?

A business relationship is one which:

- Helps in the carrying out of transactions on a frequent, habitual or regular basis and
- Where the total amount of any payment to be made is not known, or capable of being known, at the outset.

Just because your customer is a business does not mean you have a business relationship with them. A business relationship is when you treat a customer in a different way than the way in which you treat your one-off customers.

How will I know if the customer wishes to establish a business relationship?

You must ensure that you obtain sufficient information about the nature of any new business you deal with, including the amounts of money involved and the expected frequency of transactions. At the first transaction, you should establish the:

- Reason for establishing the business with you,
- Nature and level of the activity to be undertaken and
- Origin and destination of the funds.

You should also consider why the customer is using your services.

Why is evidence of identity important?

In order to follow the trail of laundered money, law enforcement authorities need to know the names of people involved.

When is identification required?

You must confirm and retain the ID of any customer who:

- Wishes to establish a business relationship with you involving frequent or regular transactions and the total value of transactions is not known at the start,
- Conducts a single transaction over £10,000 (or equivalent), or conducts two or more one-off transactions which appear to you (whether at the outset or subsequently) to be linked to other

transactions and the total amount involves, in total £10,000 (or equivalent) or more,
- Conducts any transaction that you know or suspect might involve either the proceeds of crime or is to be put to criminal or terrorist use.

Do I need to check ID for small value transactions?

You are not obliged to check ID for small value, or limited transactions unless it is within a business relationship - provided money laundering is not suspected.

From whom should I take evidence of identification?

Normally, you must take this evidence from your customer. In instances where your customer is or appears to be acting on behalf of someone else, you must obtain ID evidence from everyone in the chain.

What should I do when a customer wants to carry out a transaction that requires identification?

You should:

- Check evidence of ID at the first transaction,
- Where possible, retain a photocopy of the evidence or at the very least, record and retain information that would enable a copy to be obtained,
- Check it on a regular basis and satisfy yourself that the customer is who they claim to be.

What are the best forms of identification evidence?

The law states that you must satisfy yourself that the person is who they say they are. Because there is no single form of official ID in the UK, you should obtain a range of separate types and cross-refer them to confirm that they are consistent. Some combinations of identification are a:

- Full passport or identity card and full driving licence,
- Full passport or full driving licence and secondary identification or,
- Full passport or official identity card and secondary identification.

What if I am still not satisfied?

Where you are presented with insufficient evidence, you may decide to make additional checks by, for example, phoning a third party after asking your customer to nominate someone to vouch for them. The telephone number of the third party must be listed in the telephone directory.

If you are still not entirely satisfied with the identification presented to you, you should refuse the business and report to your Nominated Officer, who will then decide whether to pass it on to NCA.

What if the customer doesn't have a passport or full driving license?

You must satisfy yourself that the person is who they say they are by obtaining evidence to confirm the customer's identity. Acceptable alternative evidence of ID includes:

- Firearms certificate and
- Council tax bill for the current year

Documentary evidence of address includes:

- Council tax bill for the current year and
- Recent mortgage statement from a recognised lender.

In the case of asylum seekers, evidence of ID includes Forms SAL 1 or SAL 2.

This list is not exhaustive. You should take a risk-based approach, guarding against impersonation.

Provisional driving licenses are not acceptable.

What checks should I make on the document evidence given to me?

You should:

- Check the date of birth compared to the customer's appearance in the photo ID and
- Compare spellings of names and addresses on each document.

Please discuss any abnormalities found in the results with the nominated Money Laundering Registration (MLR) officer.
(see Annex: 4 for details on checks to be made)

What must I do when my customer is a company?

Where your customer or supplier is a limited company, you should identify the individuals who you deal with who have authority within that company to move funds, (not just cheque signatories) and obtain details of the company's:

- Registered number, corporate name and any trading names used,
- Registered address and any separate principal trading addresses,
- Photo ID,
- Profile check,
- Companies House check to validate the name, address and directors of the company. If the client registered is not a director of that company, then CFS-ZIPP will ask a director of that company to sign a company member additional user form. This will then give the person

that has registered authorisation to use and operate the e-account on behalf of that company.

How often should I update my customer's record of ID?

You need only update the evidence of ID if something has changed. For example, you may need to update their address details if they move. It is advisable that information held is reviewed on an annual basis, to ensure that it is still up to date/valid.
(see Annex: 4 for more information)

Record Keeping

You will need to hold all records of business transactions for at least **five years** from the date that the business relationship ends.

Why do we have to keep records for five years from the end of a business relationship?

It's the law. The purpose of keeping records is to enable law enforcement to reconstruct business transactions; often well after the original business has been concluded. In making and retaining records you should have in mind the need to provide a clear audit trail of the business you have conducted.
The records that must be kept are:

- A copy of, or the references to, the evidence of the customer's identity obtained under the customer due diligence requirements as per the regulations
- The supporting records in respect of the business relationships or occasional transactions that are the subject of customer due diligence measures or on-going monitoring.

In relation to the evidence of a customer's identity, businesses must keep the following records:

- A copy of the identification documents accepted and verification evidence obtained, or
- References to the evidence of customer's identity.

Transaction and business relationship records (for example, account files, relevant business correspondence, daily log books, receipts, cheques, and so on) should be maintained in a form from which a satisfactory audit trail may be compiled, and which may establish a financial profile of any suspect account or customer.

What is an audit trail?

An audit trail is a step by step record by which financial data can be traced to its source. In the case of money laundering the aim of establishing an audit trail is to trace the funds through to the first transaction (the placement) to identify the launderer.

What records do I have to keep?

The records that we keep must be sufficient enough to form a complete audit trail for customs officers to follow from the start of the transaction to the end; this is particularly important should the transaction later become part of an on-going investigation by law enforcement.
There are several different types of records we should keep:

- A copy of the evidence of identification presented. Photographic evidence is particularly valuable.
- Details of where the copies of identification can be found, which should be filed and easily recoverable. You must keep these records for at least five years from the date when the relationship with your customer finishes.
- Business records. You must keep a record of all transactions, regardless of whether the ID of the customer or client needed to be verified, for five years.
- All records of disclosures. Letters received from NCIS or any other correspondence with a law enforcement agency should be retained for at least five years.

Please note: We retain Individual customer & business client records for at least a five year period *after an e-account is closed.*

Identifying Suspicious Activity

Look out for any suspicious actions or activity at every dealing stage with the customer. For example, this can be an unusual remittance abroad or a transaction amount that is not in normal line of activity.

The following list provides several types of behaviour or activity that may be suspicious. The list is not exhaustive and not conclusive. Rather employees who have contact with customers, intermediaries or counterparties should use the list as a guide for inquiry and follow up:

1. The customer wishes to engage in transactions that lack business sense, or are inconsistent with the client's stated business/strategy.

2. The customer exhibits unusual concern for secrecy, particularly with respect to his identity, type of business or dealings with companies.

3. Upon request, the customer refuses to identify or fails to indicate a legitimate source for his funds.

4. The customer exhibits an unusual lack of concern regarding risks, commissions, or other transaction costs.

5. The customer appears to operate as an agent for an undisclosed principal, but is reluctant to provide information regarding the principal.

6. The customer has difficulty describing the nature of his business. The customer lacks general knowledge of his industry.

7. For no apparent reason the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

8. The customer is from, or has accounts in, a country identified as a haven for money laundering.

9. The customer, or a person publicly or known to be associated with the customer, has a questionable background including prior criminal convictions.

10. The customer account has unexplained or sudden extensive activity, especially in accounts that had little or no previous activity.

11. The customer account shows numerous currency or cash transactions aggregating to significant sums. This is however not relevant as CFS-Zipp does not have any cash transactions.

12. The customer account has a large number of wire transfers to unrelated third parties.

13. The customer account has wire transfers to or from a bank-secrecy haven country or country identified as a money laundering risk.

14. The customer account has unusual transactions or transactions that are disproportionate to the customer's known business.

If you identify suspicious activity, contact the Nominated Officer who is responsible for issuing a **Suspicious Activity Report** through the *National Crime Agency (NCA) Suspicious Activity Report (SAR)* online system. The Nominated Officer should also notify senior management.

Note: DO NOT raise any concerns with the customer or use words to suggest you are not happy with anything that may tip them off.

(see section on 'Dealing with the National Crime Agency' Annex: 1 below for more details)

Examples of Money Laundering

Money launderers use a variety of techniques to hide the movements of their laundered money. Where legal and regulatory controls are strong, launderers must make greater efforts to hide their 'dirty' money. A few examples are featured here.

Bureau De Change

A launderer may attempt to exchange small denominations of one currency for large denominations of another. Also, if the bureau's customers are occasional, this makes KYC & KYB checks more difficult.

For example: A trafficker takes large sums of drugs money and distributes them amongst 10 different people who work for him. Each person takes an amount under £10,000 to a bureau de change at different days and times over two weeks. The money is all in small denominations of Sterling and is laundered for large denominations of Euros. The money is then driven across the border from the north to the south and used partly to purchase more drugs. The workers who carried out the transactions are given small payments for their trouble, but the launderer doesn't mind this small sacrifice for clean money.

Money transmitters

Small money transmitters can be attractive to launderers as they offer lower transmission rates than banks.

Another attraction of money transmitters is the fact that the movement of money from country to country makes the audit trail harder to follow; with some of the methods used for transmission there may be hardly any audit trail at all.

For example: A launderer takes his cash to a small transmitter who keeps very few records. He hands over £9,000 in cash from drug trafficking to the transmitter and asks for it to be sent abroad. The transmitter's method for transfer involves a slip of paper with a code for the receiving person to quote to the receiving transmitter followed by a confirmation phone call between the two transmitters authorising the transfer. The coded paper is thrown away; the sending transmitter keeps no record of who the money was going to. There is no recognisable audit trail and the customer regularly makes these transactions through family and friends. The launderer therefore has a much better chance of going undetected.

Cheque Cashers

Cheque cashers are not an obvious target for laundering, as launderers do not receive cash. They receive third party cheques instead.

For example: Mr A buys an antique object using dirty money and sells it the same day at an auction, accepting a cheque as payment. He then takes the cheque to a cheque casher and exchanges it for clean money. He pays a small commission to the cheque casher, but it's worth it.
Cheque cashers can be conduits for other proceeds of crime such as tax evasion.

Anti-Money Laundering for Agents of CFS-Zipp

Who is an Agent of CFS-ZIPP?

An Agent is a company sponsored under CFS-Zipp's e-money licence which provides payment services on behalf of CFS-Zipp. Note that any e-money that is issued must be held in the CFS-Zipp designated Client Fund Account if required to be held for more than 24 hours upon initial receipt of the money. Furthermore an Agent cannot issue any e-money either, and this must be done solely by CFS-Zipp. An Agent can be a company that acts as an Issuer or Acquirer of CFS-Zipp e-money products (Ex: virtual and physical cards) or providing other e-money solutions like E-Wallets.

The fundamental requirement to fall under Agent definition will be the ownership and management of a separate "Host Platform" that will provide an account programme for customers where they can store e-money balances and access the account online.

The Host may be provided by CFS-ZIPP under licence to the Agent or the Agent may have or choose to deploy its own Host application that allows for customer e-banking operations.

Do Agents need to comply with compliance regulations?

A Compliance Officer must be appointed by the Agent and made responsible for executing processes and procedures connected with the information set out in the following section of this document.

CFS-Zipp will be available to assist the Agent in setting up its AML processes and will require the following documents in order to monitor the companies on a regular basis:

- Transaction details with the evidence of screening the customer details through the sanction lists. (details include - name, address, ID, Proof of address & beneficiaries details etc).
- Evidence of checking for Politically Exposed Persons and other AML checking during transactions.
- Reconciliation of all transactions may also be requested on a daily, weekly or monthly basis depending on the volume of transactions.

Auditing Agents

CFS-Zipp requires its Agents to submit to a quarterly Internal Audit Report (i.e. compliance audit report) conducted by a professional compliance consultant and the CFS-Zipp Compliance Team together.

The Compliance Audit should confirm the following things:

1. Completed testing of the identity of the company and organization by MLR, FSA, and Companies House Certificate and confirmed by the auditor.
2. Completed testing of CDD, EDD, Risk Assessment, F&P of the management and confirmed by the auditor.
3. Completion of the regular staff training, records and testing the standards of training and confirmed by the auditor.
4. Test report of SARs and NCA reporting system – confirmed by the auditor.
5. Testing and verification of Record keeping procedures and records.
6. Testing the Risk Assessment and management procedures.

The Agent will assist and co-operate fully with the audit team. The Agent will provide the external consultant (recommended by CFS-Zipp) access to such information, premises, personnel and equipment of the Agent as the audit team may reasonably require solely for the purposes of conducting an Audit. CFS-Zipp will also look at ways to ensure that we review the systems and process of the organisation to ensure that they remain fit for purpose. Where systems are found not to meet with the needs of the business or at worst they are not working in practice, CFS-Zipp will record the action necessary to rectify the problem and the time permitted to take remedial action.

CFS-Zipp management may require the audit team to make a further visit to ensure remedial action has been taken and systems are in place and working to the required levels.

Consequences of failing to follow CFS-ZIPP AML Guidelines

Where such Audits as above reveals a material failure, then CFS-ZIPP will impose penalties upon the Agent including but not limited one or all of the below:

i. Termination of the Agency Agreement; and/or

ii. Restrictions on the Agency's activities; and/or

iii. Stipulate remedial measures to be taken which shall be immediately implemented by the Agent; and/or

iv. Financial penalty; and/or

v. Full costs of such Audit if any

The effectiveness of the AML Procedures is dependent on all employees/intermediaries following the basic rules. This document outlines the procedures for Agents to follow identifying new customers and customer transactions in line with the Anti-Money Laundering (AML) regulations.

AML and Compliance Procedures for Agents

Know the Persons Dealing with Your Company

All Agents must ensure that they collect and verify relevant Know Your Customer (KYC) or Know Your Business (KYB) information/documentation from all individuals and businesses that register for and operate financial accounts or enter into financial provision activities with the Agent

Monitor Activity

At all times CFS-Zipp's Agent's employees should be alert to questionable activities, such as large transactions and wire transfers, as well as to high volume and seemingly inconsistent transactions.
If the Agent is not using the CFS-Zipp provided Host, it must ensure that the following reports are generated and analyzed on a regular basis:

- Accounts with a total transaction value that exceeds £10,000 or equivalent, or
- Where the total number of deals exceeds 10 per day

The Agent will periodically review customer account activities to determine if any existing account exhibits the risk factors for suspicious activity outlined in the AML Guide.

E-account activities should be monitored at all times to ensure that the Agent:

- Requests written evidence from the customer if the dealing limit exceeds £10,000,
- Performs end-of-day deal checks to see if all activities are in line with our expectations,
- Checks all deposits to see if the remitter(s) are known to us. If the member name does not appear on a deposit, then the deposit is held in a suspense e-account and only allocated to the member's e-account once verified,
- Undertakes a monthly check of unusual dealing activity and document this activity in a report.
- Where appropriate, enhanced monitoring of particular accounts is undertaken, including all government official and public figure

accounts and high net worth accounts for foreign persons, if such accounts exist.
- Reviews existing accounts against new notices, bulletins or additions to the list of countries, entities or individuals on the OFAC and other relevant web sites (such as HM Treasury, FATF and FinCEN) to determine if any current customer appears on those lists and to take appropriate action if a match occurs.

Each Employee of the Agent is also expected to bring to the Agent's Compliance Officer's attention any customer activity, transfers or patterns of activity that appear unusual or that could indicate money laundering activity.

The Compliance Officer is responsible for;

- Investigating suspicious activity referrals to determine if the Agent should require additional information to enhance account monitoring or notify CFS-Zipp who will notify regulatory authorities if appropriate.
- Consulting with service providers to the Agent to determine whether these service providers make available compliance reports to assist with the monitoring of accounts for anti-money laundering compliance.

Reporting Suspicions

Anti-money laundering processes require a team approach. Money laundering issues are complex. The Compliance officer of the Agent should not attempt to sift through them alone and if the officer becomes aware of any suspicious circumstances, or have any questions, the officer should promptly consult with the Nominated Officer of CFS-Zipp.

Suspicious activity reports – internal company process

In the situation that an employee, agent or agent employee (for this purpose, collectively, staff members) has suspicions about a customer and/or transaction, he must ensure that the company MLRO is notified about his suspicions as soon as possible.

Staff should use the internal 'Suspicious Activity Report Form'.
The SAR should contain as a minimum the following information:

- Date/time of transaction
- Amount
- Customer name/customer ID information (e.g. passport number, etc)
- Transaction number
- Reason for suspicion of transaction

If in doubt, the staff member should call the MLRO to discuss the reasons for their suspicion – however, they should be careful not to do this whilst the customer is standing in front of them (they may 'tip off' the customer otherwise, see below).

In the situation where the staff member works for an agent, the report should be made in the first instance to the Agent MLRO, who must then report on to the CFS-Zipp's MLRO.

The timing for submitting the internal SAR is important. The law states that an individual working in the regulated sector should make a report as soon as he or she becomes suspicious. This may mean either before the transaction takes place or immediately afterwards.

Where a staff member becomes aware that a customer wants to carry out a transaction which is suspicious and the timing for the transaction allows it, the staff member must ensure that 'consent' is given before processing the transaction. 'Consent' means that the company has sought and obtained approval from the Financial Intelligence Unit at the National Crime Agency

(NCA) to process the transaction. Further information on 'seeking consent' is provided below.

However, staff may decide that there would be a danger that if they were to seek consent for a particular transaction (i.e. in advance of the transaction taking place) that there might be a danger that the customer would be 'tipped off'. See below for more information on 'tipping off'.

All staff members will have fully discharged their duties, and will have the full protection of the law, once a report of their suspicions has been made to the company MLRO.

Once the MLRO receives the internal SAR from the staff member, the MLRO has two options:

- Report the SAR on to National Crime Agency (see procedure below)
- File an internal note indicating why, on the basis of review of the circumstances around the transaction, it is judged not necessary to make a report to NCA

The MLRO should complete the MLRO SAR Resolution form (see appendix for sample) in the event he decides not to make a report to NCA

Dealing with the National Crime Agency

The Financial Intelligence Unit within NCA, which was created on 3 April 2006 by the National Crime and Police Act 2005, runs the disclosure regime for money laundering and terrorist financing. It is a law enforcement body devoted to dealing with organised crime within the UK and networking with other law enforcement agencies to combat global organised crime. For full details on NCA and their activities view their website at: http://www.nationalcrimeagency.gov.uk/

Making a Suspicious Activity Report to NCA

A suspicious activity report (SAR) is the name given to the making of a disclosure to NCA under either Proceeds of Crime Act or the Terrorism Act. NCA has issued a preferred form to be completed when making a SAR, which may become mandatory in the future. NCA encourages firm to start using the preferred form now.
Preferably, firms should use SARs Online (http://www.nationalcrimeagency.gov.uk/) where you have computer access. This securely encrypted system provided by NCA allows firms to:

- Register the firm and relevant contact persons
- Submit a SAR at any time of day
- Receive e-mail confirmations of each SAR submitted

SARs can still be submitted in hard copy, although they should be typed and on the preferred form. Firms will not receive acknowledgement of any SARs sent this way.

Hard copy SARs should be sent to: Fax: 020 7238 8256 or by post to: UK FIU, PO Box 8000, London SE11 5EN. The Financial Intelligence Helpdesk can be contacted on 020 7238 8282. Firms can contact NCA on this number for:

- Help in submitting a SAR or with the SARs online system
- Help on consent issues
- Assessing the risk of tipping off so you know whether disclosing information about a particular SAR would prejudice an investigation

NCA is required to treat any SARs confidentially. Where information from a SAR is disclosed for the purposes of law enforcement, care is taken to ensure that the identity of the reporter and their firm is not disclosed to other persons.

It is our company policy that only the MLRO can submit a SAR to NCA.

It is expressly forbidden for employees to make a SAR direct to NCA.

Seeking 'Consent'

Staff may encounter situations when processing a transaction where a request needs to be made to NCA 'seeking consent' to undertake acts which would be prohibited as a principal money laundering offence. The idea behind consent is that the company is seeking a permission to proceed with the transaction before the transaction is finally processed.

NCA has up to 7 days to confirm whether or not the transaction for which a consent has been requested can proceed – until NCA give consent, the transaction cannot proceed – it is frozen. In these circumstances, the staff member must be very careful that they do not 'tip off' the customer about the reason for the delay in processing the transaction.

Where NCA gives notice that consent to a transaction is refused, a further 31 day period (the "moratorium") commences on the day that notice is given. The 31 days include Saturdays, Sundays and public holidays. It is an offence to undertake the act during this period as the participant would not have the appropriate consent. The moratorium period enables NCA to further their investigation into the reported matter using the powers within Proceeds of

Crime Act (POCA) in relation to the criminal property (e.g. imposing a restraint order). If the moratorium period expires and no such action has been taken, the reporter is free to proceed with the act(s) detailed in the initial disclosure.

It is company policy that all requests for consent must be processed through the company MLRO – it is expressly forbidden for employees to make a 'consent' request direct to NCA.

'Tipping Off'

Any staff member needs to make a judgment as to whether any delay to the transaction ('consent request') would have the effect of 'tipping off' the customer.

It is a criminal offence under POCA Part 7 for anyone, following a disclosure to the MLRO or to NCA, to do or say anything that might either 'tip off' another person that a disclosure has been made or in any way prejudice an investigation. The Terrorism Acts contain similar offences. This means that businesses must not tell a customer:

- That a transaction was/is being delayed because consent from NCA has been requested;
- That details of their transactions or activities will be/have been reported to NCA;
- That they are being investigated by law enforcement.

The punishment on conviction for 'tipping off' is a maximum of 5 years imprisonment or a fine or both. In situations where delaying a transaction may inadvertently lead to 'tipping off', it will make sense to process the transaction and then ensure that a SAR is submitted to the MLRO as soon as possible after. The staff member will have the protection of the law as soon as a SAR has been submitted to the MLRO.

If in doubt about whether to proceed with a transaction, the staff member should call the MLRO for advice.

Documentation

Supporting documentation is a cornerstone of our anti-money laundering procedures.
Unrecorded steps are soon forgotten. Records assist in tracking relevant information and in demonstrating that the company/individual has conducted

our business responsibly and with integrity. All interviews, searches and activities undertaken to verify integrity of transactions and persons must be documented and stored for reference by CFS-ZIPP and the Financial Conduct Authority (FCA) if and when required.

All records must be kept for a minimum of five years after the business relationship with the customer ends.

Annex 1: Risk Based Assessment

All Agents and the MSB customers of CFS-ZIPP are required to have a Risk Based Assessment in place. Below is a format that they may wish to follow to prepare one:

Risk Assessment of your E-Money Business

The 2007 Money Laundering Regulations require that all E-Money businesses must adopt a 'risk based approach' to its customers, products and business practices. Risk may be established both on the basis of objective criteria and subjective criteria. A 'risk rating' is given to each criterion.

Risk Ranking	Grading
Low Risk	L
Low-Medium Risk	L+
Medium Risk	M
Medium – High Risk	M+
High Risk	H

Below are summarised some of the operational risks that have been assessed and identified within our Company's business.

Country Risk - Areas of Operation

Some of the countries on the Transparency International list are detailed below using this information and the risk score indicates the levels at which EDD is followed outside normal operational factors.

Country	Risk Factors under the Corruption Perception Index from Transparency International	Risk Score	Services provided To or From
UK	This Country is ranked 16 out of 180 with a risk factor CPI of 7.7 from 10. Including the confidence rating of 7.2 - 8.1. This validates our assessment of risk as low.	L	Yes
Italy	This Country is ranked 55 out of 180 with a risk factor CPI of 4.8 from 10. Including the confidence rating of 4.0 - 5.5. This validates our assessment of risk as low -	L+	Yes

	medium.		
Spain	This Country is ranked 28 out of 180 with a risk factor CPI of 6.5 from 10. Including the confidence rating of 5.7 - 6.9. This validates our assessment of risk as low - medium.	L+	Yes
Ireland	This Country is ranked 16 out of 180 with a risk factor CPI of 7.7 from 10. Including the confidence rating of 7.5 - 7.9. This validates our assessment of risk as low.	L	Yes
Pakistan	This Country is ranked 134 out of 180 with a risk factor CPI of 2.5 from 10. Including the confidence rating of 2.0 - 2.8. This validates our assessment of risk as high.	H	Yes
Bangladesh	This Country is ranked 147 out of 180 with a risk factor CPI of 2.1 from 10. Including the confidence rating of 1.7 - 2.4. This validates our assessment of risk as high.	H	Yes

It is CFS-ZIPP's policy to consider and take note of any reports produced by the Financial Action Task Force (FATF) on ML/TF risks in relation to particular countries where available. These reports are available at: www.fatf-gafi.org.

The FATF assessments are used as an indicator – they enable us to determine when we should place closer scrutiny on the destination for payment transactions. This does not mean that customers who send to these locations are transacting illegally or are suspected of illegal activity.

Products

Our company licences enable us to carry out specific activities business and to offer all related services subject to regulatory terms and conditions being met. Our business may add in the future some or all of the service listed below (unless indicated by a value then the activity is not carried out).

Product	% of total business	Risk Ranking
E-Wallets	20%	L
E-Voucher Issuing	0	M

Merchant Services	15%	L
Technology Outsourcing	40%	L
Retail money remittance services	0	L
Wholesale payment services	0	L
High value money transfer services	0	L+
Foreign Exchange plus onward transfer	0	L+
Escrow Services	0	H
Payment Account services	0	M+
Credit card services	0	M
Pre-paid payment cards, debit cards, direct debit and standing order services	No	M
Mobile phone or fixed phone payments	0	M+
Foreign Exchange	0	L
Third party cheque cashing	0	M+
Loan products	0	M+

Transaction

How are they are processed	% of total business	Risk Ranking
'Face to Face'	10%	L
'Non Face to Face'	90%	L+

Size of Transaction	% of total business	Risk Ranking
Below £1000	50%	L
£1001 to £9999	40%	L+
Above £10000	10%	H

How are they funded?	% of total business	Risk Ranking
Non cash transactions	100%	L
Cash transaction	0	L+

Customers

Individual Customers	% of total business	Risk Ranking
In a business relationship	100%	L
Occasional customers	0	L+
One off customers	0	M

Corporate Customers	% of total business	Risk Ranking
In a business relationship	100%	L
Occasional customers	0	L+
One off customers	0	M

MSB/Payment Institution Customers	% of total business	Risk Ranking
In a business relationship	0	L
Occasional customers	0	L+
One off customers	0	M

Currently CFS-Zipp does not have any Money Transfer Businesses operating

ID Provided (retail customers/directors/owners of Agents)

Type of ID Provided	% of Customers	Risk Ranking
EU/UK Passport/driving license (photo card) plus proof of address	100%	L
Non EU Passport plus leave to remain in UK plus proof of address	0	M
Any other form of other ID ('unusual ID)	0	H

Other Characteristics

Characteristics	Risk ranking
Customer is a PEP	H
Customer is non-face to face (first transaction)	H
Customer is sanctions list match	H
Customer is sending more money than would be justified by given employment status	H
Customer is sending money on behalf of a group of other people	H
Customer is otherwise behaving in an unusual way which may be suspicious (see below)	H

Unusual Activity which may be suspicious

- Split transactions – the customer is attempting to split a large transactions into several smaller transactions to avoid obligations to provide proof of source of funds
- New customers carrying out large transactions (as opposed to regular customers)
- Regular customer is processing transactions which do match the profile of previous transactions
- Customers processing transactions who do not appear to be legitimate owners of the funds (i.e. students processing large transactions)
- Customers involved in transactions which appear to be linked to transactions processed by other customers
- Customers who cannot provide ID when requested or who provide false ID
- Customers who cannot justify source of funds when requested
- Customer is not local to the business, (but not a tourist)
- Transactions where customer is accompanied or instructed by another person who tells him what to do

Risk Matrix – high, medium and low risk customers

It is the responsibility of the Money Laundering Reporting Officer (MLRO) to oversee all transactions which are processed. They will focus attention on high risk transactions (transactions with risk rating of H).

Risk Ranking	Summary of red flags	Action of MLRO
H	Sanctions list match	Freeze transaction and report to NCA/HM Treasury
H	Customer previously reported to NCA and NCA withheld consent	Freeze transaction and report to NCA
H	Customer provides fake ID	Freeze transaction pending enhanced due diligence check
H	Customer previously reported to NCA and consent given	EDD required
H	Transaction being processed non face to face (and customer not previously identified)	EDD required
H	Customer is a PEP	EDD required
H	Customer uses unusual ID to	

	identify himself	
H	Customer is processing level of transactions incompatible with work status	EDD required
H	Customer is demonstrating unusual behavior (which may be suspicious)	EDD required
M+ or Less		No action required

Annex 2: Bribery Offences as per Bribery Act 2010 and Penalties

1. Offences of bribing another person:

   (1) A person ("P") is guilty of an offence if either of the following cases applies.

   (2) Case 1 is where—

   (a) P offers, promises or gives a financial or other advantage to another person, and

   (b) P intends the advantage—

   (i) To induce a person to perform improperly a relevant function or activity, or

   (ii) To reward a person for the improper performance of such a function or activity.

   (3) Case 2 is where—

   (a) P offers, promises or gives a financial or other advantage to another person, and

   (b) P knows or believes that the acceptance of the advantage would itself constitute the improper performance of a relevant function or activity.

   (4) In case 1 it does not matter whether the person to whom the advantage is offered, promised or given is the same person as the person who is to perform, or has performed, the function or activity concerned.

   (5) In cases 1 and 2 it does not matter whether the advantage is offered, promised or given by P directly or through a third party.

2. Offences relating to being bribed
3. Function or activity to which bribe relates
4. Improper performance to which bribe relates
5. Expectation test
6. Bribery of foreign public officials
7. Failure of commercial organisations to prevent bribery:

   (1) A relevant commercial organisation ("C") is guilty of an offence under this section if a person ("A") associated with C bribes another person intending—

   (a) To obtain or retain business for C, or

   (b) To obtain or retain an advantage in the conduct of business for C.

(2) But it is a defence for C to prove that C had in place adequate procedures designed to prevent persons associated with C from undertaking such conduct.

(3) For the purposes of this section, A bribes another person if, and only if, A—

(a) Is, or would be, guilty of an offence under section 1 or 6 (whether or not A has been prosecuted for such an offence), or

(b) Would be guilty of such an offence if section 12(2)(c) and (4) were omitted.

(4) See section 8 for the meaning of a person associated with C and see section 9 for a duty on the Secretary of State to publish guidance.

(5) In this section—

"Partnership" means—

(a) A partnership within the Partnership Act 1890, or

(b) A limited partnership registered under the Limited Partnerships Act 1907, or a firm or entity of a similar character formed under the law of a country or territory outside the United Kingdom,

"Relevant commercial organisation" means—

(a) A body which is incorporated under the law of any part of the

United Kingdom and which carries on a business (whether there or elsewhere),

(b) Any other body corporate (wherever incorporated) which carries on a business, or part of a business, in any part of the United Kingdom,

(c) A partnership which is formed under the law of any part of the

United Kingdom and which carries on a business (whether there or elsewhere), or

(d) Any other partnership (wherever formed) which carries on a business, or part of a business, in any part of the United Kingdom, and, for the purposes of this section, a trade or profession is a business.

Penalties

(1) An individual guilty of an offence under section 1, 2 or 6 is liable—

(a) on summary conviction, to imprisonment for a term not exceeding 12 months, or to a fine not exceeding the statutory maximum, or to both,

(b) On conviction on indictment, to imprisonment for a term not exceeding 10 years, or to a fine, or to both.

(2) Any other person guilty of an offence under section 1, 2 or 6 is liable—

(a) On summary conviction, to a fine not exceeding the statutory maximum,

(b) On conviction on indictment, to a fine.

(3) A person guilty of an offence under section 7 is liable on conviction on Indictment to a fine.

[For details:
http://www.legislation.gov.uk/ukpga/2010/23/pdfs/ukpga_20100023_en.pdf]

Annex 3

CFS-ZIPP will ensure that the following factors are considered by its Agents during their daily operation at all time:

Customers applying for an E-Wallet Account

As these customers are regular/fixed, their account will require at least a standard level of due diligence at the outset. A Merchant E-Wallet account should only be opened once all due diligence documents are collected, including but not limited to:

1) Completed Merchant E-Wallet Application Form and Signed T&Cs
2) Company Incorporation Documents
3) Certified copies of Director IDs and Proofs of Address
4) Proof of Business Address
5) ID and Proof of Address for all shareholders holding more than 10% shares (in order to determine ultimate beneficiary)
6) Letter from company confirming who will be allowed access to the online E-Wallet platform

For individual account holders within the Merchant E-Wallet, the following due diligence documents are to be collected prior to account activation:

1) Basic details like name, date of birth, residence address, gender etc
2) Copy of one form of National ID
3) Copy of one form of Proof of Address

Once the individual account holder has crossed an overall transaction limit of GBP 10,000 (or the local equivalent), an additional form of National ID and proof of address may be requested as part of enhanced due diligence.

All these details are to be cross-referenced on all relevant watch lists and be checked for their identity on an independent database.

Further types of checking that can be conducted, if you are not satisfied, include:

- Requesting certified ID (ID can be certified at a post office, notary, accountant or lawyers) plus a certified proof of address
- Telephone contact with the customer at a home (land line) telephone number or business address which has already been verified, using call

to verify additional aspects of personal identity information already provided during application process
- Sending a letter to the customer at his home address and then calling him to verify details included in the letter

Please note, the easiest way to get certified customer ID is to use the 'Identity Checking service' at the UK post office (the fee for this service is £6.95.) For more details see:

http://www.postoffice.co.uk/portal/po/content1?catId=63400715&mediaId=105000818

Changes and modifications to client's details

All customers should be made aware that information is held for 5 years as per FCA guidelines – random checks may be made on information supplied and if any details are incorrect, customers will be suspended from the system until the customer supplies the updated personal information. Staff should particularly take care to make sure that customer ID information previously supplied is still valid (and that ID documents have not expired). Any customer address information provided should be re-verified at least every twelve months.

Offering services to migrant workers

Details of document required by migrant workers are available at http://www.migrantworker.co.uk/ and Home Office website: https: //www.gov.uk/ government/organisations/home-office. Firms are not required to establish whether an applicant is legally entitled to work in the UK but if, in the course of checking identity, it came to light that the applicant was not entitled to do so, the deposit of earnings from employment could constitute an arrangement under the Proceeds of Crime Act.

Due Diligence – Agents

Before beginning any business with the Agents of CFS-Zipp, the following documentation must be obtained from each Agent:

- Completed Application Form
- Signed Agency Agreement
- Confirmed Agency status with the FCA

- Full name, registered number and registered address
- Proof of Business address
- Description of Business activity
- Directors ID proofs and proof of address
- Confirmation of all beneficial owners (anyone who owns or controls, directly or indirectly, more than 10% of the company)
- Letter from the directors confirming which named individuals have authority to act on behalf of the company
- Turnover of the business, its size and number of employees
- Length of establishment
- Latest Annual Return
- AML Policy if relevant
- Organisational Structure Chart
- Extract from appropriate company register
- Certificate of Incorporation
- Memorandum and Articles

The company will confirm the following information for each agent prior to commencing business. This will include:

- Confirmation that all directors/owners/key operational staff are 'fit and proper'
- A check to ensure agent credit worthiness
- Confirmation that a nominated officer/MLRO has been appointed to supervise the compliance procedures within the agent
- Confirmation that all relevant staff within the Agent are receiving the proper AML training.
- All agency staff must read the compliance manual and undertake to ensure that procedures set down in the manual are followed in day to day operations

If agents are used, all information on originating agents will be recorded (see appendix vii) along with baseline information on the volume of transactions expected.

As recommended by the Financial Action Task Force (FATF), the company will undertake a specific risk assessment of all agents both prior to commencing business and on an on-going basis. The risk assessment will be carried out (and recorded) with reference to the following criteria. These are as follows:

- Agents conducting an usually high number of transactions with another agent location,
  Particularly through an agent in a geographic area of concern.

- The transaction volume of the agent, either overall or relative to typical past transaction volume.
- Agents that have been the subject of negative attention from credible media or law enforcement enquiries.
- Agents that are not in compliance with internal policies and external regulation, such as compliance programme requirements, monitoring, reporting, or Know Your Customer practices.
- Agents that are unwilling to follow compliance program review recommendations, and therefore subject to probation, suspension or termination.
- Agents who fail to provide required originator information upon request.
- Agents whose data collection is lax, sloppy or inconsistent.
- Agents willing to accept false identification.
- Agents willing to enter identification into records that contain false information, non-existent addresses that would be known to be non-existent to a person in that area, or phone numbers that are used as fillers.
- Agents with a send-to-receive ratio that is not consistent with other agents in the locale or is consistent with participation in a criminal transaction corridor.
- Agents whose seasonal business fluctuation is not consistent with other agents in the locale or is
- Consistent with participation in a criminal transaction corridor.
- Agents whose ratio of questionable or anomalous customers to customers who are not in such groups is out of the norm for comparable locations.

Linked Transactions

It will be company (Agents of CFS-Zipp included) policy that transactions are 'linked' when the following criteria apply:

- The same customer transferred EUR 15,000 (or local equivalent) or more in the last three months to the same receiving customer in a number of individual transactions (or EUR 5,000 within one month)
- Three sending customers or more are sending to the same receiving customer (or receiving address or receiving telephone number) AND the receiving customer or bank account has received more than EUR 15,000 (or local equivalent) in last 3 three months (or EUR 5,000 within one month)

- A sending customer is sending funds on behalf of one or several people

In the event that 'linked' transactions are identified, they should be notified to the MLRO who will determine whether or not there are any suspicious circumstances which mean the transaction should be reported to NCA.

Beneficial ownership

Corporate clients or Merchants

All corporate clients will be required to indicate when they register with the company who is the beneficial owner(s) of that company (those holding 10% or more share of the company).

invoice payments

In cases where the company is requested to make invoice payments to third parties, the MLRO will take steps to understand and record:

- Who is the owner of the invoice?
- Who is the payee of the invoice?

Both the invoice owner and invoice payee will be subject to a sanctions list check.

Source of Funds – When To Verify

Any customer will be requested to provide written proof of source of funds for any one off transaction of EUR 5,000 (or local equivalent) or more.

Acceptable proofs will include:

- Source of funds declaration
- Mini statement
- Bank statement less than three months old
- Letter of secured or unsecured loan
- ATM receipt
- Wage slip
- Or other acceptable document

In the event that the customer is unable to provide any of this information, the transaction must be refused.

Alternatively, the transaction can proceed if the customer provides a banker's draft, a bank counter cheque or if funds come from a bank account in the name of the sending customer.

If any customer does cumulative transactions which total more than EUR 10,000 (or local equivalent) in any 12 month period, then he will be asked to provide written confirmation of proof of address plus documentation of source of funds. A failure to do so will be regarded as suspicious and a report should be made to NCA.

Annex 4: Politically Exposed Persons Check

The definition of 'PEP' is set out below:

- Is or has, at any time in the preceding year, been entrusted with prominent public functions
- Is an immediate family member of such a person
- Is a known associate of such a person
- Is resident outside the UK
- Is or has, at any time in the preceding year, been entrusted with a prominent public function by –
- a state other than the UK;
- The European Community; or
- An international body; or
- Is an immediate family member or a known close associate of a person referred to in the paragraph immediately above.

It is a matter of company policy that all customers will be required to indicate whether they or any member of their family has previously worked in a non - EU country at any time in the preceding 12 months. In case the answer is yes, then further enquiries must be made to establish whether the customer may meet the criteria for being 'politically exposed'.

In cases where PEP is identified:

- Senior management approval should always be sought **before** establishing a business relationship with a PEP
- The source of funds should be established

The business relationship should be subject to enhanced and constant monitoring.

Establishing the source of funds

It is important that before a business relationship is entered into with a PEP their source of funds is established and CFS-Zipp is satisfied that there are no indications that funds that will be used for transactions to be carried out are derived from corruption (i.e. receipt of bribes), fraud or an attempt by the PEP to remove/hide assets from their home country.

The source of the PEP's funds may be established by asking the individual concerned a series of questions to determine from where they receive their money. These questions could include confirmation of the main source income (i.e. salary), any business interest or investments from which funds are/will be received.

Making a decision to transact with the PEP

In order to satisfy itself, below are areas on which questions can be asked of the PEP to determine whether a business relationship should be established- information from this can be presented to Senior Management of CFS-Zipp for them to make an informed decision:

- What is the position and the duties of the PEP- (please note that a less 'senior' PEP is less of a risk than heads of states, MP's, members of the Judiciary, Ambassadors)
- Are there any family members/close associates that are PEP's also?
- Identify the customer and the beneficial owner of the account.
- Know the customer's country of residence.
- Know the objective of opening the account and the volume and nature of the activity expected for the account.
- Obtain information on the occupation and the other income sources.
- Obtain information about the direct family members or associates who have the power to conduct transactions on the account.

Currently CFS-Zipp is not transacting with any PEPs.

Annex 5: Suspicious Activity Report Format

SAR No: ...../.....

Particulars	Remarks
Date:	
ID of the customer:	
Name/address of Customer:	
Telephone no of Customer:	
Nature of suspicious activity:	
Give full detail of suspicion: [Include detail of transactions and identity checks.]	
Attach any relevant documents: 1. Transaction receipts 2. Proof of ID and Address 3. Sanctions list checks	
Name of the Reporting Officer:	
Signature by Reporting Officer:	
Refer to SOCA: [To be completed by MLRO]	
Do not refer to SOCA: Reason for decision: Details	
Signature by MLRO:	
Date referred to SOCA:	

Approved By: ....., MLRO on _____