Max Express LLC
AML/CTF Policy

Contents

1. Scope and Purpose

This policy has been created by and for the use of Max Express LLC and its Members which include directors and board members of Online Service Solutions S.A., employees, Contractors providing specific services including but not limited to software installation, vendors and agents (the "Members"). All this policy can be freely used by the Members.

This manual is designed to be used in two ways. Initially it is aimed to provide the general reader with an understanding of proceeds of crime and anti-money laundering issues affecting Max Express LLC and the actions to be taken to manage or reduce those risks and the responsibilities of the businesses employees.

Secondly it is to be made available as a reference point where any employee can turn to find out what they need to be doing in any given set of circumstances.

The general guidance provided to all employees is that where suspicious activity or unusual behaviour by customers in relation to their interactions with the business is suspected or known then this must be brought to the attention of the Money Laundering Reporting Officer (MLRO).

All Members are required to acknowledge and adhere to this policy

It is the policy of Max Express LLC that all activity will be undertaken with due regard to law, regulation and guidance in respect of dealing with the proceeds of crime and anti-money laundering. The Money Laundering Reporting Officer is responsible for this policy.

2. Introduction

Crime damages society by undermining lawful activity. It takes many forms including primary offences such as theft and fraud. Legislators have long recognised that, to tackle acquisitive crime (where property including money is taken or lost), it is not just the initial offenders that need to be dealt with. Targeting those who create a market for stolen property, or provide outlets to clean stolen assets will eventually make the primary offences less profitable and attractive.

Society is also at risk from terrorism. All terrorist activity requires funds to maintain it as an entity, to drive its promotion and to deliver on their operations in the form of terrorist attacks. Globally it is known that terrorist groups raise funds through criminal activity. Those funds require laundering in order to retain their value and make them useable to each specific cause.

All commercial business is susceptible to inadvertently receiving or dealing with the proceeds of crime and the vast majority of this will be in the form of money. But specific businesses have been listed as those with an increased responsibility for recognising their increased risk of being associated with handling the proceeds of crime or money laundering. Those businesses are either financial institutions or the gambling industry.

3. General responsibilities

Staff:

- Board of Directors – oversee the Proceeds of Crime/Anti-Money Laundering/Counter Terrorist Financing regime.
- Executive Management - to review and approve the Proceeds of Crime/Anti-Money Laundering/ Counter Terrorist Financing regime.
- Money Laundering Reporting Officer (and Deputy MLRO in the absence of the MLRO) – to design and oversee the Proceeds of Crime/Anti-Money Laundering/Counter Terrorist Financing regime, receive reports, make enquiries, disclose to authorities, implement due diligence, record keeping and staff training and keeping updated on legislative changes.
- Management – to add perspective to any reported suspicions from Employees.
- Employees – to be observant and report suspicions.

Corporate:

In addition to the normal requirements of our regulators we are also required to report any key events to the relevant regulatory authorities within 5 working days of being aware of such an event.

A key event is any event which could have a significant impact on the nature or structure of a licensee's business.

Definitions

4. What are the proceeds of crime?

The proceeds of crime are, in the main, any money or assets derived from any criminal activity. It will be obvious that money obtained through theft, robbery, burglary or fraud falls into this category. However, money obtained by selling stolen goods, drugs, counterfeit goods would also be included. Additionally, anyone concerned in arranging or assisting to do any of these things and profiting from them will also be dealing with the proceeds of crime. It covers handling the benefits of crimes such as theft, fraud, tax evasion and terrorism.

5. What is money laundering?

Money laundering is the term given to the ways criminals hide or attempt to hide where the proceeds of crime come from. More simply this is described as trying to turn funds obtained from or through criminal activity into "clean" money.

There are three steps in the process:

Placing	-	Putting criminal money into a legitimate business
Layering	-	Moving the money around, for example between games and services
Integrating	-	Taking the money that now appears clean, out and using it legitimately

It must be noted that spending the proceeds of crime is equally classed as money laundering. Where someone is playing normally they are still considered to be money laundering where the money used is originally from a criminal source. A "good customer" is only such if their source of funds is legitimate. If it is not, then they are putting you and the company at risk.

6. What is terrorist financing?

Terrorist financing covers all the activity conducted by terrorists or their support networks by which they raise funds. The overall intention of Government and regulators is to make it harder for terrorist networks to operate by reducing the resources available for propaganda, recruitment, facilitation, training, and support of families, as well as harder for extremists to mount attacks.

In real terms the gambling industry may be utilised by terrorist support networks as a facility for the storing or transferring of funds from one place to another by international transfer of funds or the transfer of funds between individuals, for example by chip dumping (the deliberate losing of a game in order to pass funds to another customer) during a game of on-line poker.

7. What is suspicious activity?

Suspicious activity is extremely difficult to define succinctly. It is about the subjective view of an individual or a set of circumstances that are either unusual or curious to the observer. Suspicion will only arise where, following curious or unusual event(s), we have investigated the circumstances and possibly questioned those involved /concerned to explain the event(s). Weighing up that explanation will allow us to determine if that activity is plausible or suspicious.

Another way of describing suspicious activity is activity that the reporter believes, or suspects, is related to the spending or use of the proceeds of crime or money laundering activity and as a result must be reported.

Other things that may raise our curiosity could include a sudden change in the customer's pattern of gambling activity such as those identified within the Moneyval 2013 Report below:

- Information provided by the costumer contains several mismatches (e.g. email domain, telephone or postcode details do not correspond to the country);
- The registered credit card or bank account details do not match the customer's registration details;
- The customer is situated in a higher-risk jurisdiction or is identified as being listed on an international sanctions list;
- The customer is identified as a politically exposed person;
- The customer seeks to open multiple accounts under the same name;
- The customer opens several accounts under different names using the same IP address;
- The source of funds being deposited into the account appears to be suspicious and it is not possible to verify the origin of the funds;
- The customer logs on to the account from multiple countries;
- A deposit of substantial funds followed by very limited activity;
- The cutomer has links to previously investigated accounts;
- Different customers are identified as sharing bank accounts from which deposits or withdrawals are made.

An email or Enhanced Customer Due Diligence (ECDD) Report is sent by employees/managers to highlight curious activity that upon investigation becomes suspicious.

8. What is a suspicious activity report (SAR)

Curiosity about events will occur on a frequent basis in daily life at home and at work. In the work environment, when we become curious about an incident, we should investigate it or raise it to the attention of a supervisor to investigate. Where it cannot be reasonably explained away then formal reporting should be considered. A suspicious activity report is the formal notification sent by the MLRO to external authorities.

In the report details of the time, date, persons involved and person reporting should be included. There must also be a narrative description of the activity. The narrative will clarify if the activity is the behaviour of an individual, a transaction of finances or a pattern of behaviour or transactions (give reference numbers if appropriate to help with any investigation). It should detail the activity without resorting to jargon. Subsequent readers of the report may have no link or understanding of the gaming or digital environment and so in house phrases may need to be avoided or explained.

Frequently narrative sections of reports can be long to include as much detail as possible. This is perfectly acceptable but writers are encouraged to use short sentences to make the information as readable and understandable as possible.

Finally, and often missed, is a clear explanation of what was actually suspicious. Again this should be written so that a person outside of our business can actually understand what has aroused our suspicion and cause them to think what needs to be done to deal with the matter.

9. When is a customer in a business relationship

A customer is deemed to be in a business relationship as soon as they have registered for play and made an initial deposit of funds into an account. As soon as we have established a business relationship then we are duty bound to carry out Customer Due Diligence (CDD) i.e. to record identification verifying who the customer is.

A business relationship is one that you enter into with a customer where both of you expect that the relationship will be ongoing. It can be a formal or an informal arrangement.[1]

There is then a further requirement to seek Enhanced Due Diligence (EDD) if the customer plays consistently to the levels described in section 20 of this policy.

10. What is meant by 'Consent'?

As a business that holds customers' funds in accounts there will be occasions where customers may be subject to suspicious activity reports in relation to their ownership or handling of potentially laundered or otherwise stolen money. If this occurs the customer's account must be suspended. A SAR must be submitted to the MLRO. The MLRO will then submit the SAR to the appropriate authority and seek 'consent' to do a prohibited act.

Prohibited acts will include the returning of funds to the customer.

Consent can take up to seven days to be granted. Nothing may be said to the subject of the 'consent' request about the submission to the appropriate authority as this would constitute the offence of tipping off which is covered in more detail below.

Where 'consent' is not granted then the MLRO will advise on any action to be taken.

11. What is a High Risk Customer?

All customers from high risk jurisdictions as identified by FATF; any customer highlighted as part of a sanctions regime as well as any customer suspected of being a PEP or any customer highlighted due to suspicious activity.

12. What is a politically exposed person?

A Politically Exposed Person (PEP) is an individual who has, or has had at any time, a prominent public function or who has been elected or appointed to such a function in a country or territory.

This makes the definition very wide ranging. PEPs include:

- Heads of state or heads of government;
- Senior politicians and other important officials of political parties;

- Senior government officials;
- Senior members of the judiciary;
- Senior military officers; and
- Senior executives of state owned body corporates.

In addition immediate family members of people in the above list are PEPs. Immediate family includes spouses, partners, children, siblings, parents in law, and grandchildren. Close associates of people in the above list are also classed as PEP's. Close associates include someone who is widely known to maintain a close business or professional relationship with such a person and people who are in a position to conduct substantial financial transactions with such a person.

The fact that a person is a PEP does not automatically mean that they are involved in money laundering or terrorist financing. It is however something that results in an alteration to that person's risk profile and causes them to be subject to additional customer due diligence measures.

Where a PEP is identified through our Customer Due Diligence or Enhanced Customer Due Diligence processes this will be brought to the attention of the MLRO who will (in the first instance) prepare a report for the Compliance Department (who will decide as to whether we should continue the business relationship and if so what additional monitoring may or may not be required). The Chief Operations Officer (COO) is also to be notified for information purposes. If additional monitoring is required they will state what that monitoring should be, by whom it should be done and how it should be recorded or whether it is best, in the interests of the business to terminate that relationship.

13. Offences

As this area of business is heavily legislated and regulated, it is only to be expected that there are a number of criminal offences that can be committed. The main offences are listed below with an explanation of each and examples where these offences may be committed.

Concealing criminal property (S.327 Proceeds of Crime Act 2002)
This offence is committed where a customer brings to us money they have obtained through crime and we conceal it, disguise it, convert it, transfer it or remove it from the UK. Where we may be seen to do this is where we deal with a customer, whose activities are suspicious, and we fail to report it to the authorities, or we do so and do not take the opportunity to cease trading with them. Converting it may be described as the process where we allow them to play a deposit almost down to nothing then play it up into winnings which appear to be lawfully obtained. If you are found guilty of such an offence you could suffer a penalty of up to 14 years' imprisonment, a fine or both.

Arranging to facilitate acquisition, retention or control of criminal property (S.328 Proceeds of Crime Act 2002)
This offence may be committed by those within a gambling company where suspicious activity has taken place and an account is established for that customer. Our management of that account would be deemed to be either retaining or controlling the criminal property. If you are found guilty of such an offence you could suffer a penalty of up to 14 years' imprisonment, a fine or both.

Acquisition, use or possession of criminal property (S.329 Proceeds of Crime Act 2002)
A gambling company commits this offence where a customer is playing with stolen or suspected stolen money and the company profits from that business relationship. If you are found guilty of such an offence you could suffer a penalty of up to 14 years' imprisonment, a fine or both.

Failure to disclose –Regulated Sector (S.330/1 Proceeds of Crime Act 2002)
This relates to all employees working within the regulated sector. The regulated sector includes all banking and financial institutions but also includes remote gambling. Remote gambling has the widest possible definition in that it is any business holding a gambling operating licence and so covers all their particular business. All the MAL activities may be seen to fall within this remit. Where suspicious activity is seen then it must be reported to the

MLRO. The MLRO is then responsible for reporting suspicious behaviour onto the appropriate authorities. If you are found guilty of such an offence you could suffer a penalty of up to 5 years' imprisonment, a fine or both.

Tipping off (S.333 Proceeds of Crime Act 2002)

A person is guilty of an offence if they makes a disclosure to any person that they have been made the subject of a suspicious activity report. In effect this means that we should not discuss this with anyone outside of those directly involved that a report has been made to a MLRO or onward to police or the appropriate authority. This does not prevent any person from asking a customer about any suspicious activity they may have seen. It only requires that no mention is made of having reported it to the MLRO or beyond.

If the person did not know or suspect that telling the customer about the disclosure would prejudice any investigation then there is a defence in law. In reality it would appear that to commit this offence there would need to be a deliberate act by a person intending to ruin a police investigation before any form of prosecution could be contemplated. If you are found guilty of such an offence you could suffer a penalty of up to 5 years' imprisonment, a fine or both.

IMPORTANT:

Tipping off therefore does not apply if the customer is given the impression that you are possibly suspicious about a transaction because you are asking questions about the source of funds. The priority is always to protect the company and concerns about tipping off should never prevent anyone from asking necessary questions to ensure a customer or their source of funds is genuine.

Therefore, a clear example of tipping off would be to tell a customer that we had reported their activity to the FIU.

14. Legislation and references

There are many documents that impact upon Max Express LLC management of proceeds of crime and anti-money laundering issues. The following list records those that currently shape our activity and are recorded here for reference.

- Proceeds of Crime Act 2002
- Money Laundering Regulations 2007
- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations 2012
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism
- Regulation of the Minister of Finance of 21 of September 2001 on determination of the sample register of transactions, the method of its maintenance and the mode of submitting the data from the register to the General Inspector of Financial Information
- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism

Processes

15. Reporting suspicious activity

Where any employee identifies suspicious activity they should always report the matter. Initially the matter should be raised with their line manager who may help to determine if the event itself is innocent or can otherwise be explained without casting unnecessary suspicion upon the customer.

Where the matter is satisfactorily explained and there are any outstanding notes, these should be updated to reflect there is no longer an open question or suspicion.

Where suspicion is aroused then the matter should be brought to the attention of the MLRO either directly or through the line manager.

The MLRO will determine whether to suspend the account (for customers) or refer an employee or business relationship to senior management pending a decision on continuance of the business relationship.

16. Role of the Money Laundering Reporting Officer and their Deputy

The MLRO receives all reports of suspicious activity. The MLRO will review each suspicious activity report and will decide if it is appropriate for the matter to be submitted to the authorities.

Where there is insufficient material to justify a submission externally, or the matter is to be reported but the suspicion is tenuous, then the MLRO may require the original reporter to continue to monitor the activity of the customer and submit subsequent reports to be assessed.

If the suspicious activity reported amounts to a strong indication that the customer, staff member or business partner/affiliate is dealing with the proceeds of crime, or is money laundering or developing funding for terrorist activity, then the MLRO will instruct a termination of the Business Relationship.

In cases where the suspicious activity reported is found to be weak or unjustified the MLRO will look to provide additional training on a specific or generalised basis.

17. Customer monitoring

In cases where the MLRO receives a suspicious activity report relating to a customer, they may decide that there is currently insufficient information on which to base a case for lodging a suspicious activity report with the appropriate authorities. Where there is still an element of curious behaviour that cannot be explained, the MLRO may ask the reporter and their manager to continue to monitor the financial and gaming activity of the customer. In requesting monitoring the MLRO shall specify either a time period or a specific number of visits during which the monitoring should take place. At the end of that monitoring a record should be made of the further observations and this must be resubmitted to the MLRO. The MLRO should then decide whether to progress the report or note that no further action is required.

18. Customer due diligence (CDD)

All customers who are in a Business Relationship will have certain due diligence checks carried out at the commencement of that relationship.

For a customer to join our e-wallet system there are three distinct phases:

- Registration
- Account creation

- Deposit

On registration a geographical location check is carried out. This is a check on the customer's computer IP address to ensure the customer is in a permitted jurisdiction. If the customer is not from a permitted jurisdiction, the customer will be told they are not permitted to register on the site.

The details required upon registration are title, first name, surname, date of birth, country, home address, phone number, email address, username, password and currency. These are all mandatory fields.
A customer account is then created. Each account will hold the customer's personal details and a log of their financial transactions and game activity. Unlike a traditional financial account it does not allow an overdraft or credit and does not generate interest or any financial gain.

We will then carry out our own internal check which looks for duplicate accounts. The check is on customer names, date of birth and postcode. If multiple factors are the same then account is considered duplicate and the matter is reviewed by the Fraud team.

If a customer account passes all checks it will be set to "Opened", then the customer is asked to set a payment method and given the deposit page in order to make their first deposit. If the customer decides to deposit later, he will have to login to the site, go to the deposit page and make his first deposit.

If identity is verified, there are no restrictions on the customer account.

In the event that the monitoring identifies an incident, a member of the Fraud team will investigate and record the outcome in Black list.

Where a customer's activity on their account appears to amount to suspicious behaviour, additional checks will be performed.

19. Enhanced Customer Due diligence (ECDD)

Enhanced Customer Due Diligence is to be carried out when:

- Single or aggregate deposit within a period of time hits a threshold
- High risk business relationships are identified
- Potential PEP is identified

The Fraud team will perform simplified Customer Due Diligence background checks on the Customer and, if anything suspicious detected, escalated to the MLRO.

The same level of ECDD will not be carried out for every customer. Where a customer has only just hit the criteria for ECDD set out above a review of their activity will take place. It may be quickly established that they have recently won a similar amount in gaming on line with us. However, where a customer frequently deposits large amounts per month then this will be worthy of deeper investigation and potentially require consideration for a personal discussion with the customer to seek their proof of funds or wealth.

Enhanced customer due diligence checks can be conducted in three ways.

- Open Source searching
- Due diligence search through private companies
- Customer interview

Open Source Searching

Background checks can be carried out using "Open Source" searching. This will involve a member of the Fraud team searching through internet search engines against the data provided by the customer. The strength of this system is that it is relatively cheap and quick. The weakness is that there are such a wide variety of search engines and data sets that reliable information can be hard to find and even when found will normally need some form of corroboration to support it. In addition this will be a one off search and so only provide a snapshot in time rather than providing ongoing searches.

Customer Interview

The strongest and best means of achieving due diligence information is to speak directly (either by phone or email) with the customer and request documentary evidence or proof of the source of their funds/wealth.

Where a customer is asked to provide proof of the source of their funds or wealth then the following items will provide legitimate evidence:

- Proof of employment
- Pay slips
- Letter from solicitor
- Letter from accountant
- Proof of winnings from other gambling company (e.g., proof of lottery win)
- Media coverage relating to personal wealth

This list is not exhaustive. The person checking will need to satisfy themselves that the documentation is bona fide which can be done through open source searching or by contact with the originator of the document.

For some time there has been a fear that contacting customers and directly asking for this information will lead to a loss in customers who wish to have their privacy respected. There is clearly a need to use sensitivity when asking what many customers consider personal questions.

Information is provided to help customers understand why such questions may be asked and to help speed up the process this can be sent to the customer in advance. We should also explain that as part of our due diligence we may request documentary evidence to identify source of funds and to explain that due diligence (DD) is a requirement of all operators. Specific training and guidance material is available for appropriate team members to advise on the best techniques to use when seeking EDD information without causing offence.

However many customers are becoming aware that there is a need to provide this information in order for the business to comply with its obligations. Whilst there is room for sensitivity and understanding, those customers who consistently refuse to answer questions or provide the necessary information will effectively make their circumstances appear more suspicious and so may lead staff to submitting a suspicious activity report. If they continue to refuse or otherwise not co-operate, the MLRO will have no choice but to end the business relationship (see section 23).

20. Risk assessments

An overall business risk assessment is completed on an annual basis and is the subject of review of the Board of Directors and the MLRO. This assessment is a record of the actions taken to minimise or mitigate risk that the businesses have adopted as a norm, on customer registration, during play and as and when an incident occurs. This last point relates to suspicious activity being identified or notification of suspicion from an outside source, such as a data protection request being received pursuant to a criminal investigation.

Guidance from the regulators advises that there are five specific factors that need to be assessed for risk. These are the customer, the product/service, the delivery channel and the jurisdiction.

The Customer

The customer's risk is identified and addressed at registration. This is covered in the section on Customer Due Diligence above.

The Product/Service

This is reviewed as part of the Business Risk Assessment prior to the registration of a customer and is the subject of on-going review within the quarterly Business Risk Assessment meetings.

The Delivery Channel

In this area there are only two channels which are described as online and mobile. The risks of this being targeted for proceeds of crime, money laundering or terrorist financing have been undertaken and are documented in the ICS

21. Data subject access requests

From time to time law enforcement or other State-backed bodies may make requests for personal data relating to specific customers. Such requests will also be received from private companies, private individuals or even the customer themselves. All such requests once confirmed as genuine should be forwarded to the Compliance Department

Where the request is made Legal will determine if the request is proportionate, lawful, appropriate and necessary before releasing the data.

Where the request highlights the fact that the information is required because the subject concerned is involved in possible criminality then the MLRO is to be informed and with the involvement of Compliance will review the matter further and make a recommendation as to whether we should terminate the Business Relationship. In doing this

they may liaise with the other departments and individuals to ensure that this action will not cause significant harm to any person or significant loss to/damage of property.

22. Terminating Business Relationships

There will be occasions where Max Express LLC will need to consider the termination of a Business Relationship with a customer. This is most likely where the customer's activity is seen to be suspicious and is subject of a SAR. In these cases it will be correct to terminate the Business Relationship in order to reduce the risk of offences being committed.

Where notification is received that a customer may be concerned in criminal activity, or be the subject of a live police investigation the question of termination of the Business Relationship will need to be considered.

In each of the above cases the MLRO and if needed in consultation with the Compliance Department and COO, will make the decision and notification of that decision to the appropriate manager.

23. Record keeping

All activity relating to suspicious activity will be recorded and retained for 5 years after the relationship ends.

Enhanced customer due diligence enquiries and results will be recorded and will be retained for 5 years after the relationship ends.

24. Changes to the Policy Manual

The MLRO is responsible for regularly reviewing this policy and ensuring that the contents are up-to-date and fit for purpose. The MLRO is responsible for ensuring that all employees who should be aware of, and familiar with, the contents of this policy are so aware. The Training department will maintain a register of all who have been made aware of the contents of this manual and policy and any updates as part of the AML/Compliance training.