ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Payroll Agents

Sector Specific AML/CFT Guidance Notes

September 2021

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Contents

1. Foreword 4
2. Introduction 5
2.1 National Risk Assessment 6
3. Risk Guidance 6
3.1 General Higher Risk Indicators 6
3.2 Red Flags 8
3.3 Risk factors specific to the sector 9
4. Customer due diligence 10
4.1 Who is the customer? 11
4.2 Source of funds 11
4.3. Ongoing Monitoring 12
5. Case Studies 13
5.1 Financial management of a criminal organisation 13
5.2 Tax evasion 1 13
5.3 Tax evasion 2 14
5.4 Ghost employees 14
5.5 Payroll Company Fraud (Tax Fraud) ("PCF") 15

Version history

Version 2 (September 2021)	Updates to reflect changes to the main structure of the AML/CFT Handbook Updates to footnotes to include links in the main body for consistency purposes Updates made to links in relation to the updated NRA 3 – updates to risk indicators 5 – additional case study

1. Foreword

For the purposes of this sector specific guidance, the business of a payroll agent refers to a business conducting activity included in paragraph 2(6)(k) of Schedule 4 to the Proceeds of Crime Act 2008 ("POCA"). The activity is defined as follows:

2 Business in the regulated sector

(6) This sub-paragraph applies to -

(k) subject to sub-paragraph (10), a payroll agent as defined in sub-paragraphs (7), (8) and (9)

(7) For the purpose of (6)(k) "**payroll agent**" means a person who is involved with the payment of earnings to, or for the benefit of, any individual.

(8) Sub-paragraph (7) applies where the payroll agent is not the individual's employer.

(9) Sub-paragraph (7) also applies where—

(a) the payroll agent is the individual's employer but the place of work of the individual is outside the Island;

(b) the work being carried out by the individual is not being carried on directly for the payroll agent or any company within a group to which the payroll agent belongs; and

(c) the work being carried out by the individual is not the principal trade or business of the payroll agent. (10) Sub-paragraph (7) does not apply to a technical service provider who only provides services which support the provision of payroll services and at no time takes possession of the funds being transferred.

For the purpose of this sub-paragraph **"technical service provider"** means a person who supports the provision of payroll services by providing services including –

(a) the processing and storage of data;

(b) trust and privacy protection services;

(c) data and entity authentication;

(d) information technology and communication network provision; and

(e) the provision and maintenance of terminals and devices used for payroll services.

To provide additional clarification in relation to who would be classed as a payroll agent; where a business processes the payroll calculations, collects the funds from an employer/business, pays the net proceeds to the employee/contractor and arranges for the payment of withheld taxation to the relevant authorities this would be considered the business of a payroll agent as defined above even where the employee / contractor is based outside the Island.

Where a business is purely involved with the calculation of wages and the calculation of any associated deductions and tax liabilities (such as ITIP / VAT / NI) but does not enter into the possession of funds, this activity falls in line with the aforementioned technical service provider definition and therefore this business would not be considered to be a payroll agent as defined by the Act. However, where a business is undertaking any form of calculations relating to tax it should consider whether it would be classed as a "tax advisor" (activity included at paragraph 2(6)(j) of Schedule 4 to POCA) or "external accountant" (activity included at paragraph 2(6)(i) of Schedule 4 to POCA).

By virtue of being included in Schedule 4 to POCA, the business of a payroll agent is subject to the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code"). Also, this sector is included in the Designated Businesses (Registration and Oversight) Act 2015 which came into force in October 2015. The Financial Services Authority ("the Authority") has the power to oversee this sector for Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") purposes.

2. Introduction

The purpose of this document is to provide some guidance specifically for the payroll agent sector in relation to AML/CFT. This document should be read in conjunction both with the Code and the main body of the AML/CFT Handbook ("the Handbook").

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the sector and provides further guidance in respect of approaches to customer due diligence where it may vary across sectors.

There is not yet a published typology paper in respect of this sector from the FATF. Therefore the risk factors within this document are based on the following FATF reports regarding accountants as some of the risk factors are common across both sectors.

- Risk Based Approach for Accountants
- Guidance for a risk based approach – Accounting profession

Due to common overlaps in the provision of payroll services with those of tax advisers or accountants, the Authority recommends that relevant persons familiarise themselves with these documents, and any other relevant documents published concerning the payroll,

accounting or tax advisory sectors. Also, some case studies are included to provide context to the risks of the sector.

2.1 National Risk Assessment

The Island's National Risk Assessment ("NRA") was published in 2015 and was updated in 2020. Payroll agents must ensure their business risk assessment (and customer risk assessments where necessary) take into account any relevant findings of the NRA.

Payroll agents could be vulnerable to ML/TF in a number of ways, including the creation of "ghost" employees/contractors by fraudsters using either real or fabricated personal details. The NRA sets out the main risks and vulnerabilities in further detail.

The level of risk for ML is assessed as medium for payroll services due to the factors identified in the NRA and considering the comparative size of the sector in the IoM and existing typologies. There are currently no typologies in respect of the use of payroll agents for TF; payroll does not appear to be a preferred route for TF and therefore the risk of TF is assessed as medium low.

3. Risk Guidance

The ML/FT risks of a payroll agent will vary for each business based on a wide range of factors such as the type of products they supply, their customers and delivery channels. The services of a payroll agent may be used by money launderers to provide an additional layer of legitimacy to the criminal's financial arrangements, especially where the sums involved may be larger.

Vigilance should govern all aspects of the business' dealings with its customers and payroll activities, including:

- customer on-boarding;
- customer instructions;
- transactions into and out of customer accounts;
- ongoing monitoring of the business relationship;
- technology / security issues if there is an online element to the business relationship;
- any outsourced / delegated services; and
- risks of internal fraud/ML or abuse of systems to facilitate or enable ML/TF for others

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed in chapter 2 of the Handbook, the following activities may increase the risk of the relationship. Just because an activity / scenario

is listed below it does not automatically make the relationship high risk, the customer's rationale / nature / purpose of the business relationship etc. should be considered in all cases.

If a business is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concerns, it should be determined whether this is suspicious or unusual activity. Please refer to chapter 5 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 of the Code:

13 Ongoing monitoring

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;

(b) conduct EDD in accordance with paragraph 15; and

(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and

(b) make an internal disclosure.

This list of higher risk indicators is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. Also please see the list of red flags included at 3.2 of this document.

- Where a customer is reluctant to provide normal information or provides only minimal information.
- Where a customer's documentation cannot be readily verified.
- The customer is reluctant to provide the business with complete information about the nature and purpose of the relationship including anticipated activity.
- Where there are difficulties in confirming the customer's business or in verifying the customer is part of the claimed business or supplying services to that business
- Where the payment chain is complex and the relevant person is not directly dealing with the customer business and their employees, or not directly dealing with contractors and the end user recipient of their services
- The customer is located in a high risk jurisdiction.
- Transactions involving numerous jurisdictions.
- The customer is reluctant to meet personnel from the firm in person and / or uses a "front person".

- The customer has no discernible reason for using the business' services, or the business' location.
- The customer has a history of changing businesses and using a number of businesses in different jurisdictions.
- The customer's address is associated with multiple accounts that do not appear to be related.
- The customer is known to be experiencing extreme financial difficulties.
- The nature of activity does not seem in line with the customer's usual pattern of activity.
- The customer acts through intermediaries such as advisers in order not to have their identity registered.
- The customer exhibits unusual concern with the business' compliance with Government reporting requirements and/or AML/CFT policies and procedures.
- Requests for payments to be made to third parties rather than the customer/or payments to be made to an account which differs from that previously used and verified
- Payments received come from an unknown account/account not verified as belonging to the customer or employment agency in the supply chain
- Requests for wire transfers / payments to be sent to, or originate from higher risk jurisdictions without apparent business reason.
- The customer's transaction pattern suddenly changes in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.

3.2 Red Flags

In addition to the above higher risk indicators, there are some factors that are likely to be "red flags" in relation to that particular relationship and would therefore usually be suspicious activity. If a relevant person identifies suspicious activity appropriate steps as explained in section 3 of this document, and the Code, must be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information;
- where it is identified a customer provides suspicious identification documents;
- the customer is evasive when asked for details regarding the underlying employees/contractors;
- the customer does not provide the business with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated activity;
- the customer is secretive / evasive when asked to provide more information;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;

- the customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect;
- the customer enquires about how quickly they can end a business relationship where it is not expected;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for;
- the customer is known to have criminal / civil / regulatory proceedings against them for crime, corruption, misuse of public funds or is known to associate with such persons; and
- the customer is interested in paying higher charges to keep their identity secret.

3.3 Risk factors specific to the sector

The following section of the guidance covers some of the risk factors specifically related to this particular sector. Further guidance surrounding the risk assessments is outlined in chapter 2 of the Handbook.

The Code mandates that a number of risk assessments are completed -

- business risk assessments (paragraph 5)
- customer risk assessments (paragraph 6)
- technology risk assessments (paragraph 7)

Considering the technology risk assessment specifically, this must estimate the risk of ML/FT posed by any technological developments, such as the use of online delivery channels or payments being made in virtual currencies), to its business. An assessment should be undertaken whenever a relevant system is introduced or changed.

Payroll agents can be vulnerable to money laundering in a number of ways. Some examples are below.

- Where services include the handling of clients' funds, the payroll business may provide services that help legitimise the proceeds of a crime, or help legitimise the incorrect calculation of deductions (tax evasion) by processing payments.
- The UK National Crime Agency's document Indicators of Modern Slavery and Human Trafficking in the Accountancy Sector highlights Payroll services amongst accountancy type sectors exposed to Modern Slavery and Human Trafficking exploitation.
- Criminals establishing themselves as both employer and employee/contractor (either directly or through an associate) the proceeds of crime are "paid by the employer" to the contractor using fabricated invoices or timesheets. This can be identified by

establishing source of funds, and undertaking reasonable due diligence on both the employer and the employee/contractor including the source of funds and monitoring the relationship. (Also risks of internal facilitation in the payroll business creating employer/employees on systems).

- The creation of "ghost employees/contractors" within a company, which refers to someone on the payroll who doesn't actually work for the company. The ghost employee/contractor is frequently a recently departed employee/contractor, a made-up person, or friend or relative of the fraudster. The payroll agent could be used to make payments to this "ghost". The payroll agent must therefore be vigilant in relation to the amounts of the payroll, number of employees/contractors, any variations to this information. (Again there is a risk of internal facilitation or fraud.)
- Unnecessary steps or entities are introduced in the supply/payment chain to allow insertion of criminal proceeds by money launderers who then receive "clean" funds from the supply/payment chain, or to facilitate tax fraud in the chain where the entity introduced as responsible for tax to be paid fails to make payment and is replaced by another similar entity
- Payroll service businesses should exercise care that they are not in receipt of the proceeds of proceeds of crime, bribery or corruption. Again, this can be identified by undertaking due diligence and taking reasonable measures to verify the source of funds.
- Payroll service providers should also take reasonable care to ensure that they are not abused for tax offences which is a predicate offence for money laundering.

4. Customer due diligence

Part 4 of the Code requires relevant persons to undertake customer due diligence and ongoing monitoring in relation to all business relationships. Chapter 3 of the Handbook provides guidance on how to identify and verify the identity of the customer in relation to both a natural and legal person. Also, guidance on the timing of identification and verification of identity is provided. For details of particular concessions which may be applicable please see chapter 4 of the Handbook.

In all cases where the requirements of Part 4 of the Code cannot be met (Paragraphs 9(9), 10(5), 12(11)) the procedures and controls must be provide that –

(a) the business relationship must proceed no further; (b) the relevant person must consider terminating[1] the business relationship; and (c) the relevant person must consider making an internal disclosure.

[1] In relation to a New business relationship (paragraph 8) the business relationship must be terminated.

4.1 Who is the customer?

There are two main payroll business models operating on the Island:

1. A payroll agent that provides a payroll service (calculations / deductions / payments) to another business in relation to that business' underlying employees.

   In relation to this business model the customer will be the business that has approached the payroll agent to provide a payroll service in respect of its employees. (The underlying employees that are receiving payments are not the customer.) Whilst the underlying employees are not the customer, the payroll agent will need to hold certain information on the employees in order to make payments, this can also assist the payroll agent identify if the relationship appears legitimate.

2. A payroll agent that provides a payroll service (calculations / deductions / payments) to contractors. In this case the payroll agent will invoice a third party company for the services provided to it by the contractor. The payroll company will subsequently pay the contractor for the services being provided and will retain any fees due to it for the services. Where a model such as this is used by a contractor the payroll agent must be clear regarding the rationale for this.

   In relation to this business model, and depending on contractual and commercial obligations, the payroll agent may be supplying services to either or both the contractors and the third party company.

The requirements of the Code such as risk assessments, customer due diligence (including source of funds), ongoing monitoring, record keeping etc. would apply to the customer. The Handbook provides further information in relation to how to meet these Code requirements. Where there is a variation in the business models referred to above, and it is unclear who the customer is, we would recommend discussing this further with the Authority and seeking legal advice.

4.2 Source of funds

Paragraph 8(3)(e) of the Code requires the taking of reasonable measure to establish the source of funds for all new business relationships.

8 New business relationships
(e) taking reasonable measures to establish the source of funds, including where the funds are received from an account not in the name of the customer —

(i) understanding and recording the reasons for this;

(ii) identifying the account holder and on the basis of materiality and risk of ML/FT taking reasonable measures to verify the identity of the account holder using reliable, independent source documents, data or information; and (iii) if the account holder is assessed as posing a higher risk of ML/FT, satisfying the requirements in paragraph 15.

Please see section 3.8 of the Handbook for further details on source of funds and source of wealth. Payroll agents will be receiving funds to pay the salaries/fees owed by the employer or end user and also disseminating those funds to the employees/contractors they are arranging payments for.

Where the customer is the employer whose payroll is provided by the payroll agent, it is expected that the source of funds would typically be from the customer themselves, and their activity (rather than the work conducted by the employee/contractor).

In more complex supply chains, funds may be received from, or payments made to other parties in the chain rather than directly from employers to employees, or from end users to contractors. One example might be where the end user obtains contractor services from an employment agency, and the employment agency is invoiced by, and pays funds to the payroll agent business for the work done by contractors.

If the funds are being received from a third party (including an employment agency as above), the business must identify and verify the identity of this third party where necessary. It should also seek to establish the relationship between the customer and the third party and consider the rationale for the payment and whether this appears reasonable.

In the cases of a direct wire transfer or a cheque payment the means through which the funds are transferred is self-explanatory. There are instances where payments are made, such as by BACS, where the sender information is not ordinarily attached but is available upon request the business does not have to hold that information file, however must to be able to obtain it within 7 business days of a request from a competent authority.

4.3. Ongoing Monitoring

Due to the nature of the services provided by payroll agents, in particular the numerous transfers of funds that are taking place, the ongoing monitoring provisions of the Code are of particular importance. The ongoing provisions include checking and refreshing risk assessments, transaction monitoring and customer due diligence information.

In relation to transaction monitoring, the payroll agent must ensure that the payments being made on behalf of the customers are monitored (e.g. volume, amount, jurisdiction, frequency, etc.) and it should be ensured that they are satisfied the activity is in line with the customer's risk assessment, source of funds and expected activity etc. Particular attention

should be paid to transactions which are large, complex or unusual and further action taken if necessary (such as an internal disclosure) as required by the Code.

Section 3.4.6 of the Handbook provides additional detail in relation to ongoing monitoring. Also, when undertaking the payments, the payroll agent must ensure it considers the higher risk indicators set out in part 3 of this document.

5. Case Studies

The typologies below are some examples of risks that could crystallise and cause losses and/or sanctions (civil and criminal) against the business:

5.1 Financial management of a criminal organisation

A law enforcement operation identified an accountant, J, who was believed to be part of the criminal organisation involved in money laundering and re-investment of illicit proceeds derived from drugs trafficking led by X. J's role was mainly that of a "financial consultant". His task was to analyse the technical aspects of the investments planned by the organisation and identify the most appropriate financial techniques to make these investments appear legitimate from a fiscal stance. He was also to try, as much as possible, to make these investments profitable. J was an expert in banking procedures and most sophisticated international financial instruments. He was the actual financial "mind" of the network involved in the re-investment of proceeds available to X. J operated by sub-dividing the financial transactions among different geographical areas through triangle transactions among companies and foreign credit institutions, by electronic transfers and stand-by credit letters as a warrant for commercial contracts which were later invested in other commercial activities.

5.2 Tax evasion 1

A Chartered Accountant provided services to clients whereby the income they derived in Australia was transferred into overseas bank accounts operated in an off shore banking centre in the name of the companies based there (the chartered accountants husband acted as nominee director and shareholder). The money sent offshore was recorded as business deductions in the accounting records of the clients, from which the chartered accountant prepared and lodged income tax returns. The offshore banking centre companies were administered by an accountant based in the jurisdiction. The money sent offshore were then returned to Australia via the chartered accountant's trust account, disguised as loans from the off shore banking centre based company to the chartered accountant clients, and used for private purposes, such as real estate purchases.

This alleged scheme offered the client the benefit of obtaining their income tax-free and afforded them the opportunity to claim interest payments as tax deductions. These "back to

back loans" included the fabrication of loan agreements and other accounting records to support the loans.

Foreign companies were also used by the chartered accountant's clients for the purpose of share trading in the name of the company, thereby hiding capital and/or trading profits and dividends received as a result of the share trading.

Another service provided to the clients of the chartered accountant involved the creation of personal superannuation funds to allow clients early access to retirement benefits.

Preserved superannuation benefits, belonging to clients of chartered accountant, were deposited into the chartered accountants trust account and labelled an investment from the fund to an off-shore banking centre based company incorporated by her husband. The funds were then forwarded from the chartered accountants trust account to a financial institution in the name of the individual who was a member of the fund.

This scheme allowed early access to preserved superannuation benefits to the members of the fund well before retirement. Clients of the chartered accountant also made payments to an off-shore banking centre -based company for services which were not provided by the company. This effectively provided a tax deduction for the client, to which the client was not entitled.

5.3 Tax evasion 2

A large company, Company X, developed its own in-house payroll system in order to pay its own employees. Company X then began offering the use of the system to contractors for a fee. These individuals would have a contract arrangement with Company X to cover the payment of wages but would be working (via a contract) for a third party company. The contractor would inform Company X each month the number of hours they had worked and Company X would invoice the third party company for those hours. The third party company would pay Company X the appropriate amount including the appropriate National Insurance contribution, Company X would then pay the individual a certain amount in the form of a loan. It subsequently came to light that individuals were failing to pay the appropriate tax / National Ins as their payment was being disguised as a loan rather than a salary.

5.4 Ghost employees

Note: This case study is more relevant for an entity operating its own payroll but nevertheless it is useful to highlight how a payroll system could be abused.

Mr X an employee of a large non-profit organisation created a number of "ghost employees" on the payroll system. He made up the names for these employees and used the social security numbers of people who had recently died.

Over time Mr X began entering false wage information for the ghost workers. At the same time he arranged for their pay checks to be direct-deposited into his own bank account, based on his own dealings with the financial institutions he knew the bank did not match the employee name to the one on the bank depositor's account. The payroll disbursements had to be approved by a supervisor, Mr X prepared a fake payroll summary (rather than the report from the system) and as he was seen as an exemplary employee the supervisor did not check his work carefully and failed to notice the difference in typeface from a real report.

Mr X then had to create a phony file copy of the ghost's pay checks, the office's hard copies of the legitimate pay slips were printed in yellow by the accounting department, Mr X's were printed in white. Eventually, during an audit, a white pay check was singled out and was traced through the system and the fraud was uncovered. Over the course of two years Mr X had embezzled $112,000 from his employer.

(This methodology can also be used by criminals who create a "ghost" employer, end user or employment agency, and payments are made to associates or "ghost" employees/contractors. Routing payments through a genuine payroll company or agent helps launder criminal funds and adds an air of legitimacy to monies received by associates.)

5.5 Payroll Company Fraud (Tax Fraud) ("PCF")

PCF in its simplest form occurs when a business transfers staff, along with payroll responsibilities, to a fraudulent entity (the payroll company) who supply the staff back to the business at a cost roughly equivalent to gross wages plus VAT. The payroll company pays the staff but fails to remit the Income Tax, National Insurance contributions and VAT to the authorities. There may not always be the transfer of a permanent workforce; however, when PCF occurs, there are two ever-present factors: a supply of labour; and the non-remission of taxes by an entity in the supply chain.

Models of the fraud include the following.

- A more complex supply and payment chain where the original employer (or genuine agencies) pay the employees net salaries, but contractually pass payments equivalent to tax and National Insurance amounts to entities further down the chain who are on paper responsible for paying tax and National Insurance amounts over to the tax/National Insurance authorities. (The fraudster company sits further down the chain.)

- Supply chains involving contractors or sub-contractors (for example security guards or agency nurses) provided through employment agencies where the contractors provide their services as normal, and receive net pay from the employment agency, but the company responsible for paying over tax and National Insurance etc. is further down the chain and does not remit the monies.