


Document Title	Financial Crimes Policy	
Approved by	Group Finance Director	
Date approved	31 October 2024	
Review date	30 October 2025	

FINANCIAL CRIMES POLICY

1. POLICY STATEMENT

The Group is committed to the highest level of ethical behaviour and has **zero tolerance** for tax evasion, facilitation of tax evasion, failure to prevent facilitation of tax evasion, money laundering, terrorist financing, proliferation financing, fraud and the failure to prevent fraud. Any such practices are strictly forbidden, and we are committed to preventing them.

- 1.1. We expect all employees and associated persons to be able to identify and take steps to prevent any scenarios where there may be a risk.
- 1.2. As a group, we support the questioning and eventual declining of business where there are any suspicions of Financial Crimes.

2. DEFINITIONS

The following definitions are used in this Policy:

CBRN	Means chemical, biological, radiological or nuclear.
EDs	Means the executive directors of Lucy Group Ltd
Group or Group Entity	Means Lucy Group Ltd and all entities controlled by, or under common control with Lucy Group Ltd.
Financial Crimes	Means tax evasion, facilitation of tax evasion, failure to prevent facilitation of tax evasion, money laundering, terrorist financing, proliferation financing, fraud and the failure to prevent fraud.
NCA	Means National Crime Agency
Nominated Officer	Is responsible for the Group's compliance with the Financial Crimes legislation and for advising Workers on concerns pertaining to Financial Crimes.
POCA 2002	Means the Proceeds of Crime Act 2002.
SAR	Means suspicious activity reports.
SMT	Means the senior management team of the applicable Group Entity
TA 2000	Means Terrorism Act 2000
Workers	Means individuals in the Group working at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, apprentices, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, or our agents, distributors, representatives, suppliers or any other person working with any Group Entity, wherever located.

3. SCOPE

- 3.1. This Policy applies to all Workers.
- 3.2. Compliance with this Policy is mandatory. Any Worker who knowingly fails to comply with the requirements of this Policy, including its appendices will be the subject of disciplinary proceedings, which may result in summary dismissal. Such behaviour may also be reported to the relevant authorities, and you may commit a criminal offence if you fail to comply with this Policy.
- 3.3. We reserve the right to terminate contracts with any suppliers, contractors, agents, distributors, business partners, joint venture partners and third-party representatives who are unwilling, unable, or fail to act in a manner consistent

with this Policy.

- 3.4. If you have any questions on this Policy, please contact your line manager or the Group Finance Department.

4. RESPONSIBILITY

- 4.1. The EDs are responsible for the Group's compliance with Financial Crimes legislation and the Company Secretariat will act as the Group's Nominated Officer, unless they delegate this to someone else. The email address for the Company Secretariat is Secretariat@lucygroup.com.

4.2. The EDs:

- 4.2.1. take the lead within the Group on Financial Crimes matters; and
- 4.2.2. ensure our Financial Crimes efforts have appropriate oversight and engagement at the highest level.

- 4.3. The **Nominated Officer** is responsible for:

- 4.3.1. receiving and assessing SARs; and
- 4.3.2. determining whether any SAR gives rise to knowledge or suspicion (or reasonable grounds for knowledge or suspicion) that a person is engaged in Financial Crimes.

- 4.4. The **SMT** is responsible for:

- 4.4.1. ensuring their Workers comply this policy;
- 4.4.2. ensuring that their Workers proactively raise concerns they have under this policy;
- 4.4.3. determining whether a SAR needs to be submitted to the Nominated Officer; and
- 4.4.4. ensuring that there is an open culture that allows Workers to raise concerns.

You are responsible for proactively spotting and reporting any concerns relating to Financial Crimes. Failure to do so can lead to criminal penalties, substantial fines, disciplinary action and untold damage to your own and the Group's reputation.

5. RED FLAGS AND WARNING SIGNS

- 5.1. You must remain alert to the red flags and warning signs of Financial Crimes and make the sort of enquiries that a reasonable person (with the same qualifications, knowledge and experience as you) would make.

- 5.2. Appendix 1 Recognising Crime: Red Flags and Warning Signs for Workers identifies typical red flags and warning signs that may indicate that our organisation is involved in or is itself being used to commit crime and which would normally require further investigation. **These factors do not automatically mean that crime is taking place; though they should be considered red flags.** You should pay particular attention to matters where a number of factors are present. Note that criminals are always developing new techniques, so no list of examples can be exhaustive or fully comprehensive.

- 5.3. The sort of enquiries you should be making include:

- 5.3.1. is the documentation you have consistent with what you are being told and know about the background, nature or circumstances of the customer/supplier?
- 5.3.2. does this make sense?
- 5.3.3. how is the deal being financed: where is the money coming from?
- 5.3.4. how are we paying the supplier? If into an account that seems unrelated to them, why? Are they asking for cash payments?
- 5.3.5. is a third party providing the funds? If so, why and how are they connected to the customer?
- 5.3.6. how does the customer/supplier expect to benefit from the deal/matter?
- 5.3.7. where are the proceeds of the deal/matter going to—if not to the customer, why not?
- 5.3.8. who are the people behind any company?
- 5.3.9. who are the parties involved?
- 5.3.10. does the size of the transaction match your knowledge of the customer's finances and typical transaction size?
- 5.3.11. does the transaction involve the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of CBRN weapons?
- 5.3.12. is any company, individual or country involved in the transaction on any sanctioned or prohibited list?
- 5.3.13. does the transaction raise any concerns about tax being properly paid?

- 5.4. If you have any concerns, you should discuss these with your line manager or the SMT in the first instance, alternatively you can raise concerns to the Nominated Officer, or via the whistleblowing hotline – see section 10.

6. TAX EVASION AND FACILITATION OF TAX EVASION

6.1. The Criminal Finances Act 2017, introduced two Corporate Criminal Offences:

6.1.1. The failure to prevent facilitation of UK tax evasion, and

6.1.2. The failure to prevent facilitation of foreign tax evasion.

6.2. The Group must be able to demonstrate that we can prevent the facilitation of tax evasion as part of our day-to-day operations. If an “associated person” of our business criminally facilitates tax evasion, and a Group Entity is unable to demonstrate that we had reasonable procedures in place to prevent such facilitation, then the Group Entity is guilty of a criminal offence. “Associated person” is defined very widely in the legislation and includes any person (individual or corporate) who represents (or provides a service for or on behalf of) the business – employees, contractors, agents, and in certain circumstances external suppliers.

6.3. This means we expect all Workers not to engage in any activity which evades tax or facilitates or may facilitate the evasion of tax by any other person (company or individual). It does not matter whether the taxes are UK taxes or are due to an overseas fiscal authority.

6.4. Consequences for Failing to Comply

6.4.1. The consequences of prosecution for the business include unlimited fines, reputational damage and the likelihood of regulatory sanction.

6.4.2. Tax evasion and facilitation are also punishable for individuals with fines and custodial sentences.

6.4.3. The legislation applies to all taxes, personal and corporate, and includes VAT/GST or other local equivalent, Customs Duties, National Insurance Contributions, etc.

6.5. What is Tax Evasion?

Tax evasion involves the deliberate and dishonest use of illegal practices to pay the incorrect amount of tax. This could include not reporting all your income, deliberately not filing an accurate tax return, hiding beneficial ownership and taxable assets from UK tax authorities or diverting funds to hide income from local taxation authorities.

6.6. What is Criminal Facilitation of Tax Evasion?

It is a crime to deliberately and dishonestly facilitate tax fraud for or on behalf of another person. Real life examples of facilitation of tax evasion could include deliberately and dishonestly changing invoices for customers that could impact the VAT amount or assisting a supplier in not disclosing income (e.g. through making a payment into an undeclared overseas bank account) or deliberately overstating group cross-border intercompany charges where this may impact the Corporation Tax due either in the UK or overseas.

7. WHAT ARE, MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING AND WHY ARE THEY IMPORTANT TO ME?

7.1. **Money laundering** is the process through which the true origin and ownership of the proceeds of crime are changed so that the proceeds appear legitimate.

7.2. Typically, money laundering involves three stages:

7.2.1. Placement – the process of placing criminal property into the financial system (e.g. by breaking up large sums of cash into smaller amounts or by using a series of financial instruments (such as cheques or money orders) which are deposited at different locations);

7.2.2. Layering – the process of moving money that has been placed in the financial system to obscure its criminal origin (usually through multiple complex transactions often involving complicated offshore company structures and trusts);

7.2.3. Integration – once the origin of the money is disguised it ultimately must reappear in the financial system as legitimate funds (involves investing the money in legitimate businesses and other investments such as property purchases or setting up trusts).

7.3. **Terrorist financing** is providing or collecting funds, from legitimate or illegitimate sources, to be used to carry out an act of terrorism.

7.4. **Proliferation financing** is the act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, CBRN weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation.

8. MONEY LAUNDERING OFFENCES

- 8.1. The POCA 2002 establishes a range of money laundering offences:
 - 8.1.1. the principal offences;
 - 8.1.2. failure to disclose offences; and
 - 8.1.3. the offences of tipping-off and prejudicing an investigation.
- 8.2. **The principal offences**
 - 8.2.1. You will commit a principal money laundering offence if you:
 - 8.2.1.1. conceal, disguise, convert, transfer or remove criminal property from the UK;
 - 8.2.1.2. enter into or become concerned in an arrangement which you know, or suspect facilitates the acquisition, retention, use or control of criminal property for or on behalf of another; or
 - 8.2.1.3. acquire, use or have possession of criminal property.
 - 8.2.2. The principal money laundering offences carry a maximum penalty of 14 years' imprisonment, a fine or both.
 - 8.2.3. You will have a defence to a principal money laundering offence if you submit a SAR to the Nominated Officer.
- 8.3. **Failure to disclose** - Failing to make a SAR to the Nominated Officer where you know or suspect money laundering is an offence in itself which is punishable by up to five years' imprisonment, a fine or both.
- 8.4. **Tipping-off and prejudicing an investigation**
 - 8.4.1. You will commit the tipping-off offence if you:
 - 8.4.1.1. disclose that you, or anyone else has made a SAR to the Nominated Officer (or the NCA) of information which came to you in the course of business; and
 - 8.4.1.2. that disclosure is likely to prejudice any investigation that might be conducted following the SAR.
 - 8.4.2. You will commit the prejudicing an investigation offence if you disclose that an investigation is being contemplated or carried out and that disclosure is likely to prejudice that investigation.
 - 8.4.3. You will also commit an offence if you know or suspect an investigation is being or is about to be conducted and you interfere with documents that are relevant to the investigation.
 - 8.4.4. Tipping-off can only be committed after a SAR (including an internal SAR to the Nominated Officer) has been made.
 - 8.4.5. You will not commit tipping-off by discussing your concerns with or submitting a SAR to the Nominated Officer.
 - 8.4.6. All these offences are punishable by up to five years' imprisonment, a fine or both.
 - 8.4.7. The existence of these offences does not prevent you from making normal enquiries about your customers' instructions. You are able to make enquiries in order to:
 - 8.4.7.1. obtain further information to help you decide whether you have a suspicion; and/or
 - 8.4.7.2. remove any concerns that you have.
 - 8.4.8. Your enquiries will only constitute an offence if you disclose that a SAR has been made or an investigation is being carried out or contemplated.

9. TERRORIST FINANCING OFFENCES

- 9.1. Terrorists need funds to plan and carry out attacks. The Terrorism Act 2000 (**TA 2000**) criminalises both the participation in terrorist activities and terrorist financing.
- 9.2. In general terms, terrorist financing is the provision or collection of funds from legitimate or illegitimate sources; with the intention or in the knowledge; that they should be used in order to carry out any act of terrorism; whether or not those funds are in fact used for that purpose.
- 9.3. The TA 2000 establishes a similar pattern of offences to those contained in POCA 2002, i.e.:
 - 9.3.1. principal terrorism offences of:
 - 9.3.1.1. fundraising;
 - 9.3.1.2. use or possession;
 - 9.3.1.3. arrangements;
 - 9.3.1.4. money laundering;
 - 9.3.2. failure to disclose offences;
 - 9.3.3. tipping-off offences.
- 9.4. All offences carry heavy criminal penalties.

10. REPORTING SUSPICIONS

- 10.1. Our internal SAR form can be found at Appendix 2. Completing our internal SAR form is intended to make the process of submitting SARs to the Nominated Officer as easy as possible, but you do not have to use this form to make a SAR. If you would rather have an initial, informal conversation with your line manager or the SMT either to help decide whether a formal SAR should be submitted, or for help in making a formal SAR, you are very welcome to do so.
- 10.2. When should I report suspicions?
 - 10.2.1. ALWAYS and as soon as reasonably practicable. You will be required to explain any delays to the Nominated Officer.
 - 10.2.2. You can also report concerns using our whistleblowing hotline, details of which are available in the Whistleblowing Policy on the intranet. However, remember: a report to the Nominated Officer is the only way to ensure your position is protected under POCA 2002 if your suspicions turn out to be correct.
 - 10.2.3. If you are unsure whether you suspect a Financial Crime e.g. something just does not feel right with the matter, do not complete the SAR form, but instead discuss your concerns first with your line manager or the SMT and then with the Nominated Officer, who will advise whether you need to submit a SAR. We will keep a record of that discussion.
- 10.3. Discussing concerns with others
 - 10.3.1. There is nothing wrong with discussing a potential report with a line manager or the SMT rather than the Nominated Officer in the first instance. It may be that they have a better insight into the customer or the work.
 - 10.3.2. However, if you still have suspicions, you should speak with the Nominated Officer. Remember, a formal suspicious activity report (in whatever format) to the Nominated Officer is required where you decide you hold suspicions.
- 10.4. What happens after I make a SAR?
 - 10.4.1. On receiving your SAR, the Nominated Officer will consider the reasons for suspicion reported to them. They may ask you for more information. They will then decide whether an external SAR to the NCA is required. This decision rests only with the Nominated Officer, or their deputy in their absence.
 - 10.4.2. You have discharged your reporting obligations by making the internal SAR.
 - 10.4.3. You must follow all instructions from the Nominated Officer. You may work on the matter in the meantime but must not:
 - 10.4.3.1. transfer funds;
 - 10.4.3.2. take an irrevocable step in the matter (e.g. sign contracts or complete a deal); or
 - 10.4.3.3. do anything that constitutes tipping off.
 - 10.4.4. If in doubt, seek guidance from the Nominated Officer.
- 10.5. What can I tell the customer? There is very little you can tell the customer after you have submitted a SAR and you must not tell them that you have submitted a SAR. If you do you will be committing the offence of tipping-off and could be exposed to a criminal record and up to five years' imprisonment. Always speak with the Nominated Officer if you are in any doubt.
- 10.6. SARs and beneficial ownership discrepancies
 - 10.6.1. Reporting a material discrepancy in relation to beneficial ownership information to Companies House is not the same as submitting a SAR.
 - 10.6.2. If you suspect Financial Crime in a situation where you have submitted or plan to submit a discrepancy report form, you must also submit a SAR.

11. TRAINING AND AWARENESS

All employees and agents will be made aware of the law relating to tax evasion and facilitation, money laundering, terrorist financing, proliferation financing and fraud and must complete compulsory annual training on how to recognise and deal with transactions and other activities which may be related to Financial Crimes. Our zero-tolerance approach to Financial Crimes must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate thereafter.

Appendix 1. Recognising Crime: Red Flags and Warning Signs for Workers

This awareness tool identifies some typical red flags and warning signs that may indicate that our organisation is involved in or is itself being used to commit crime (e.g. tax evasion, facilitation of tax evasion, money laundering, terrorist financing, proliferation financing, sanctions offences, bribery, corruption, fraud or organised crime). These factors do not automatically mean that crime is taking place, but you should be aware of them and pay particular attention to matters where a number of factors are present. These red flags and warning signs would normally require further investigation.

The list is not exhaustive and if you have any concerns, you should raise them with your line manager or the Nominated Officer.

1. A supplier, contractor or anyone in your role within our business asking you to do something that does not match up with official documentation, for example, paying into a different account than that which is specified on the invoice.
2. You are feeling under pressure to process or approve an invoice (or make changes to our contractual terms) that you don't feel makes sense, for example in terms of changing the payment details or VAT/GST (or local equivalent) amount.
3. You receive an invoice from a third party that appears to be non-standard or customised or is different to what you expected.
4. Being concerned about the set up and/or supporting paperwork of a particular transaction that you think may not reflect the true commercial reality or fact pattern.
5. Someone asking for a favour that is not in line with your company policy.
6. You are aware of any short cuts in our supplier or customer onboarding procedures (e.g. someone you know circumventing the supplier set-up and due diligence process).
7. Someone who works for a third-party supplier offering you what seems like a discount, e.g. because they tell you they don't need to charge you VAT/GST or local equivalent - without giving a reason.
8. Someone at work (for example an employee or a contractor) claiming to have found a 'short cut' in how much tax they pay, or you are aware that tax is not being declared.
9. Someone at work (for example an employee or a contractor) claiming illegitimate expenses.
10. Any other knowledge or suspicion that anyone in our business, either in the UK or any other country, is evading or facilitating tax evasion.
11. Colluding in the evasion of, or turning a blind eye to, overseas tax evasion by globally mobile staff; for example by a failure to track locations of staff and potential tax liabilities and residence.
12. Use of cash payments.
13. There are payments to or from third parties where there is no logical connection to the customer.
14. Funds received from or sent to a foreign country when there is no apparent connection between the country and the customer.
15. Funds received from or sent to a sanctioned country and/or transactions involving sanctioned individuals or where sanctioned individuals have any control over, or involvement in, the company or transaction (see our Trade Compliance Policy).
16. Holding companies with links to sanctions targets or based in offshore jurisdictions historically linked to a sanctioned jurisdiction.
17. Use of an intermediary, agent or corporate structure not directly connected to the customer.
18. The Customer:
 - a. is excessively obstructive or secretive;
 - b. is a politically exposed person (PEP) or is established in a sanctioned country;
 - c. uses an intermediary, or does not appear to be directing the transaction, or appears to be disguising the real customer;
 - d. refuses to provide information or documentation or the documentation provided is suspicious;
 - e. is a corporate customer with an unusual or excessively complex structure;
 - f. is registered at an address that does not match the profile of the company, that cannot be located on internet mapping services or is also listed against numerous other companies or legal arrangements; and/or
 - g. is involved in the supply, purchase or sale of dual-use and sensitive goods.

Appendix 2. Internal suspicious activity report (SAR) form

This SAR form is intended to make the process of submitting SARs to the Nominated Officer as easy as possible, but you do not have to use this form to make a suspicious activity report. If you would rather have an initial, informal conversation with your line manager or the SMT either to help decide whether a formal SAR should be submitted, or for help in making a formal SAR, you are very welcome to do so.

Note that a report to the Nominated Officer (in whatever form) is the only way to ensure your personal position is protected under the Proceeds of Crime Act 2002 and the Terrorism Act 2000, if your suspicions turn out to be correct.

A record of this Suspicious Activity Report (SAR) will be kept by the Nominated Officer for at least five years.

You can use this form in every case where you know or suspect that another person is engaged in money laundering or terrorist financing, proliferation financing, bribery or corruption, fraud, slavery or human trafficking, organised crime group involvement, tax evasion facilitation, or any other criminal activity

If you are unsure as to whether you have such a suspicion, please do not use this form but instead seek guidance from the Nominated Officer.

SAR Reference Number (Nominated Officer use only):	[Insert number]
1. General (complete all sections)	
Date SAR submitted to the Nominated Officer	
Your name and department	
Lucy group entity	
SAR type (e.g. money laundering, terrorist financing, proliferation financing, fraud, bribery or corruption, slavery or human trafficking, organised crime, tax evasion or other criminal conduct)	
SAR subject (e.g. customer, supplier, employee, representative, distributor, etc.)	
Do you require consent/a defence to continue with the matter?	<input type="checkbox"/> Yes <input type="checkbox"/> No If you know or suspect that we will be dealing with criminal property in a way that may amount to a principal offence, we need to ask the NCA for a defence against money laundering.
Does this SAR relate to a previous SAR? <i>If unsure, please discuss with the Nominated Officer.</i>	<input type="checkbox"/> Yes <input type="checkbox"/> No <i>If yes, please provide details</i>
Are you aware of a known law enforcement interest in this matter? Select 'yes' if a law enforcement agency is aware of the suspicious activity and is actively investigating and please provide details	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unsure [Insert details]
2. Details of the main subject of this SAR (complete as much as you are able)	
Does this SAR relate to a suspect or a victim?	<input type="checkbox"/> A suspect <input type="checkbox"/> A victim
Is the subject of this SAR an individual or a legal entity?	<input type="checkbox"/> An individual (go to section 3) <input type="checkbox"/> A legal entity (go to section 4)
Are there any individuals or entities who are associated with the main subject?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, complete details in section 5
3. Individual	
Full name	
Date of Birth (dd/mm/yyyy)	
Gender	
Occupation	
Full address	
Address type	<input type="checkbox"/> Home <input type="checkbox"/> Business <input type="checkbox"/> Other

Is this address current?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unsure
Email address	
Telephone number	
Bank account details (UK or international)	
Any other ID details (e.g. passport, driving license, NI number)	
4. Legal entity	
Full name	
Company number	
VAT number	
Country of registration	
Full address	
Is this address current	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unsure
Email address	
Telephone number	
Type of business	
Bank account details (UK or international)	
Any other identification details	
5. Associated subjects (complete if appropriate)	
Details of any associated subjects (i.e. people or entities you believe are linked to the SAR subject and involved in the criminal activity), including identifying information as above and details of the nature of the association with the SAR subject.	
6. Details of knowledge/suspicion	
Does your knowledge or suspicion relate to a specific offence?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, please indicate, e.g. money laundering, terrorist financing, tax evasion, proliferation financing, drugs, fraud, terrorism, bribery, slavery, organised crime, other (please state)
Have you discussed your knowledge or suspicions with any person other than the Nominated Officer?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, please give details, (e.g. who, why, when, etc) Note that there is nothing wrong with discussing a potential report with your line manager or head of department rather than the Nominated Officer in the first instance. However, a formal SAR (in whatever format) to the Nominated Officer is required where you decide you hold suspicions.
What is the nature of the property you suspect is criminal property, if applicable?	<input type="checkbox"/> Money <input type="checkbox"/> Other property <input type="checkbox"/> N/A
Do you know the whereabouts of the property, if applicable?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A If yes, please provide details, e.g. in the case of money, the account details of where it is held
What is the total value of the criminal property involved? (if known)	
Are we holding any funds for the SAR Subject? If you are unsure, please speak to the accounts team.	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, insert how much.
Please set out your reasons for making this SAR in as much detail as possible E.g., who, what, where, when, how, why, etc	Include information such as: <ul style="list-style-type: none"> • the type of transaction made, e.g. if funds were sent or received, currency, date, location, etc • the account details used • if the transaction involves real estate, and, if so, the cost • financial and technical details used in the transaction
Please explain the act(s) involving suspected criminal property that you are	

seeking consent/defence for (if applicable)	
7. Further information	
Is there any further information you would like to disclose?	

Signatures and acknowledgement

Details and signature (discloser)	Discloser name: [Insert name] Discloser signature: [Insert signature] Disclosure date: [Insert date]
Receipt acknowledged	Nominated officer or deputy name and role: [Insert name and role] Signature: [Insert signature] Date received: [Insert date]

Once completed send this form to the Nominated Officer and, where practicable to do so, to the SMT.