GLOBAL
CORPORATE
SPECIALTY

AVIVA

Commercial Crime Insurance Application Form

Guidelines to help you complete this Application Form

- Failure to disclose all material information that is likely to influence the acceptance of the risk or the terms applied could affect the extent of cover provided or invalidate the insurance. If you are in doubt as to whether any information is material, it should be disclosed.
- Completing this Application Form does not bind the Proposer to effect cover.
- All answers should be given as a group response i.e. if any subsidiary or associated company to be insured has different responses these should be provided separately.
- Exposure information and risk management controls should be declared in respect of all entities, which should also fall under Your direct management control.
- Where you see this symbol (❖), please refer to the Appendix on page 9 for an explanation.

A. Details of the Proposer

Name of the Proposer	
Names of Subsidiaries/ Associated Companies to be insured	
Postal Address	
Postcode:	
Business Description	

Please complete the following for all operations to be included (attach additional sheet if required):

United Kingdom	Employee Numbers	Annual Wageroll	Annual Turnover	Number of Locations
Overseas Territories	**Employee Numbers**	**Annual Wageroll**	**Annual Turnover**	**Number of Locations**
TOTAL				

Overseas employees are understood to be those who are permanently contracted outside of the UK

B. Fraud Control Procedures

Human Resources, Outsourcing and Payroll

In respect of employees responsible for money, goods, accounts, other financial & treasury functions or computer programming operations:

1. Do you have an established policy for checking the background of job candidates prior to their being offered employment? Yes No

   If 'No', please provide details of the procedures used for vetting staff:

2. Is cover required for any activities outsourced to third party service providers? Yes No

   If "Yes", please state which activities are outsourced

3. Are wages and salaries independently checked against personnel records to ensure that there are no past or fictitious employees or excessive payments at least on a monthly basis? ❖ Yes No

B. Fraud Control Procedures

Physical Controls, Stock and Equipment Checks

4. What is the maximum value of stock, work in progress, raw materials and scrap at any one location? £

5. Do you have any "target" stocks or property? Yes No
(Target stocks include alcohol, tobacco, designer clothing, furs, jewellery, precious stones, valuable metals, works of art, antiques, scratch & top-up cards, mobile phones, electrical & computer hardware and software)

6. Please state how frequently independent physical checks are carried out on all stocks, materials and equipment held against verified records?

7. Are all locations containing stock, money and securities

   (a) connected to a maintained and working intruder alarm? Yes No

   (b) protected by controlled access during office hours? Yes No

Dual Controls

8. Are duties segregated so that no one person can complete any of the following from beginning to end:

   (a) Initiating and approving any electronic funds transfer instructions? Yes No

   (b) Opening of new bank accounts and amendment of the bank mandate? Yes No

   (c) Appointing new suppliers or awarding contracts? ❖ Yes No

   (d) The ordering, receipt and authorisation for payments of goods, materials, equipment or services? Yes No

   (e) Refunding monies, return of goods or disposal of assets above £1,000? Yes No

   (f) Loans and borrowing? Yes No

Computers/Ecommerce

9. Is your computer system protected by a secure firewall and virus detection / repair software which is regularly updated? Yes No

10. Do computer terminals automatically lock after a period of inactivity? Yes No

    If 'Yes', please advise the period of inactivity before locking: Number of minutes:

11. How frequently do you back up data?

12. Is this stored off site in a secure location? Yes No

13. Do your email server and internet service provider (ISP) use authentication methods at all locations? Yes No

Making and Receiving Payments

14. Are any cheques produced with facsimile or computer signatures? Yes No

If 'Yes', please provide details opposite of the type used and the maximum payment before an additional manual signature is required.

Type:

Max payment: £

15. Are payments ever accepted using 'Cardholder Not Present' methods where a 'PIN' is not required. i.e. customer using credit/debit card over the telephone/online? Yes No

If "Yes" please give details of any value thresholds up to which such methods are accepted:

£

16. Is the maximum sole signing limit (in respect of all employees, directors and/or shareholders) on all manually prepared cheques £5,000 or less? Yes No

17. Please confirm below all funds transfer methods used to instruct your bank/financial institution to make payment (e.g. written, telephone, electronic, facsimile).

18. For written, telephone and facsimile transfers, does the financial institution authenticate the funds transfer instruction to someone other than the initiator of the request before payment is released? Yes No

Social Engineering Fraud Controls

Having read the appendix definitions, please confirm that:

19. Staff have been made aware of "Fake President/ CEO Fraud" **as explained in the appendix** ❖ and, upon receiving any request for transfer of funds or payments by email or other means, they verify this by checking with the requestor physically in person and/or calling them or any other Senior Management using a telephone number which is previously known/designated (not relying on any contact details provided within the email itself). Yes No

20. In respect of the "Mandate Fraud" **as explained in the appendix** ❖

(a) where a request is made by a supplier or other payment recipient to change bank details on the proposer's system, the request is verified by contacting an authorised representative of the supplier or payment recipient, using contact details held on file, rather than those contained on the change instruction itself, prior to making any changes. Yes No

(b) Given the potential for phishing and/or virus infection, please confirm that you employ and review regularly a procedure for informing employees not to click on unknown links or open attachments on emails from unknown sources? Yes No

21. In respect of the "Invoice Fraud" **as explained in the appendix ❖** please confirm that when paying invoices, any variances on existing payment details are checked and verified with the payment recipient using contact details held on file rather than those contained on the invoice itself, prior to making payment. Yes No

22. In respect of the Vishing (telephone) Fraud **as explained in the appendix ❖** please confirm that:

    (a) All relevant staff are informed that their bank or the authorities will NEVER call and ask for PINs or passcodes, or request money is transferred to another account. Yes No

    (b) If any such calls are received, please confirm that these are verified by calling their bank using a separate telephone line or mobile. Yes No

23. Given the potential for phishing and /or virus infection, what is your procedure for informing employees not to click on unknown links or open attachments on emails from unknown sources?

Audit and Corporate Governance

24. Have all recommendations made by auditors regarding internal controls been adopted? Yes No

    If 'No' to the above, please provide details in the space opposite.

25. Do You have an internal audit department? Yes No

    If "Yes", how frequently are all areas audited?

C. Consistency of Controls

26. Are the loss prevention procedures detailed in Questions 1 to 29 above operative at all locations? If 'No', please provide details on a separate sheet. Yes No

D. Loss/Claims Experience

During the last 5 years has the proposer suffered a fraud, theft, burglary, robbery, or any other type of loss which relates directly to the cover provided under this policy (which has or could have resulted in a claim, whether insured or not)? Yes No

If 'yes' please provide details of the loss(es) or circumstance(s) – including but not limited to the date, location, estimated quantum of loss and any measures taken to prevent reoccurrence:

Please attach additional sheet if further space is required.

E. Previous Insurance

1. Do you currently have Employee Dishonesty or Commercial Crime Insurance? Yes No

   If 'Yes', please state current Limit of Liability and Excess. Limit £ Excess £

2. Has any insurer cancelled, declined renewal or imposed higher terms for the insurance proposed? Yes No

   If 'Yes', please provide details in the space provided.

F. The Cover You Require

Limit of Liability (Any Single Loss) – consider accumulation of loss given frauds can continue undiscovered spanning several years.	£
Excess (which we will deduct from each and every claim).	£

G. Subjectivity Conditions

The insurance cover provided by Aviva may be subject to You or Us carrying out certain actions. We will clearly state above if the insurance provided by Us is subject to You:

(1) Providing Us with any additional information requested by the required date(s).

(2) Completing any actions agreed between You and Us by the required date(s)

(3) Allowing Us to complete any actions agreed between You and Us. Upon completion of these requirements (or if they are not completed by the required dates), We may, at our option:

  (a) modify the premium

  (b) make amendments to the terms and conditions of the insurance cover

(4) Withdraw any insurance cover provided.

(5) Leave the terms and conditions of the insurance cover and the premium, unaltered.

We will contact You with our decision and where applicable, specify the date(s) by which any action(s) agreed need to be completed by You and/or any decision by Us will take effect.

Our requirements and decisions will take effect from the date(s) specified unless and until We agree otherwise in writing. If You disagree with Our requirements and/or decisions, We will consider Your comments and where We consider appropriate, will continue to negotiate with You to resolve the matter to Your and Our satisfaction.

In the event that the matter cannot be resolved We will withdraw the insurance cover.

The above conditions do not affect Our right to withdraw any insurance cover if We discover information material to Our acceptance of the risk that was not disclosed when requesting the original quotation.

H. How and why we use your information

We (Aviva), and our third parties, collect and use information (including data about health and unspent offences or criminal convictions) about you and, if relevant, somebody else covered under your policy and your vehicle(s), business and property.

We do this so we can:

- verify your identity and help prevent fraud
- calculate our risk to insure you
- calculate your price
- set up, assess and maintain your insurance contract with us
- renew and make changes to your cover
- process claims
- carry out marketing, profiling and analytics

We share information within the Aviva Group, our reinsurers (our own insurers) and specific other organisations for these purposes.

The information comes from:

- what you've already told us
- data we already hold about you (including from other quotes and policies with us)
- publicly available sources
- other organisations we trust
- data about your device, general location and how you interact with our website

We carry out a quotation search from a credit reference agency

This will appear on your credit report and will be visible to other credit providers. It will be clear it's a quotation and not a credit application by you. We do this when you ask us for a quote, when we prepare your renewal and sometimes if you change your cover so that we are able to offer you a monthly credit payment option. We use data from our credit reference agency to verify your identity, prevent fraud and carry out risk profiling which allows us to calculate your premium and payment options. For more information about your rights relating to profiling and decisions that are automatically processed such as pricing, see the Privacy Notice for this policy.

The identity of our credit reference agency and the ways they use and share personal information are explained in more detail at www.transunion.co.uk/crain. You can also check the information they hold about you.

We use automated processes to make decisions

This means our software decides whether we can insure you and on what terms, deal with claims and carry out fraud checks. For more information, see the Privacy Notice for this policy.

You have rights about your information

For more about your rights and how and why we use your data, see the Privacy Notice for this policy.

There's more detail in our Privacy Policy at www.aviva.co.uk/privacypolicy or you can request a copy by writing to us at Aviva, Freepost, Mailing Exclusion Team, Unit 5, Wanlip Road Ind Est, Syston, Leicester, LE7 1PD

Declaration

I/We declare that the information given is, to the best of my/our knowledge and belief correct and complete. If the risk is accepted I/we undertake to pay the premium when called upon to do so. I/We understand that my/our information may also be disclosed to regulatory bodies for the purposes of monitoring and/or enforcing the insurer's compliance with any regulatory rules/codes.

Signed: _____ Date: _____

Position Held: _____

❖ Appendix: Crime Application Explanatory Notes

Q.3 This question is asked due to the potential for payroll fraud. This is where an employee involved directly or indirectly with payroll inserts an additional 'ghost' employee (or inflates an existing employee's salary), paying themselves or an accomplice additional wages. This type of loss can lie undiscovered for many years and as such can grow substantially over a period of time.

Q.8c This question is asked due to the potential for 'supplier kickbacks'. This is where an employee appoints a new supplier that they often have a personal connection with (or sets up their own bogus company) and the two collude by inflating invoices and splitting the proceeds. Therefore it is prudent for a business to ensure that no single individual is able to appoint a supplier without independant due diligence and with sign-off processes in place.

Q.19 "Fake President/CEO" Fraud occurs when fraudsters impersonate a senior executive, asking a member of the finance team or a relevant manager to make an unusual, urgent and/or highly confidential payment (sometimes to an off shore account). In some instances the company's email system will have been compromised, with the fraudster having accessed and being able to send emails from the senior executive's legitimate account. Some requests are made over the telephone, often followed up with an email from the purported senior executive (with what might appear to be a genuine email address but could contain a slight variation when the fraudster has not gained access to the legitimate account e.g. using .com rather than .co.uk). It is prudent for all staff in positions of responsibility to have been trained to spot and prevent such fraudulent activity.

Q.20 Over the last few years, the crime insurance market has seen losses emanating from circumstances where third party fraudsters have purported to be a legitimate supplier/ payment recipients of an insured, and asked them to change their bank details on the insured's system. Often these requests are made on professional looking headed paper with logos etc. and frequently containing the fraudster's telephone number on the instruction itself thus duping the insured into making the changes. For this reason, accepting such requests by relying on headed paper is deemed to be a weakness in fraud risk management unless independently verified. Payments owed to the supplier are then made to that new bank account. Shortly after, when the legitimate supplier questions their non-payment, the fraud is discovered. This is often referred to as 'mandate fraud'.

Q.21 'Invoice fraud' is a similar fraud to that noted in Q.20 above. This is where a fraudster replicates or mocks up a genuine supplier's invoice, but changes the bank details at the bottom of the invoice to their own. Payment is then made to the fraudster's bank account.

Q.22 Telephone fraud (or 'vishing') is increasingly being used by criminals to deceive businesses into revealing company information or encouraging the transfer of funds into a bank account held by the criminal. Fraudster cold callers of this kind will often gain the employee's trust by telling them to replace the handset and call their bank's fraud department who will verify their story. Unfortunately it is possible for fraudsters to keep telephone lines open by not replacing the handset at their end. This fraud has variations:

- "Your account has been compromised; we need to secure your funds": The fraudster will telephone the insured, purporting to be calling from the police or their bank's fraud investigation department. They will persuade an employee that their bank account has been compromised and in order to protect the monies, all funds must be transferred to a 'secure' account, where they will be talked through an online transfer.

- "Your payment hasn't gone through": The fraudster will telephone impersonating a senior bank official, requesting that a particular payment is validated. During this call they will obtain details of genuine payments made, including sort codes, account numbers and monetary amounts. Armed with this information, the caller will then telephone later that day advising that the payments have stalled and need to be re-entered online to another account, with details supplied by the fraudster.

Important Notice

This declaration should be read in conjunction with this application form and its appendices and any risk presentation provided to Aviva Insurance by your insurance intermediary. The information contained therein has been used to calculate the premium, terms and conditions of the quotation. It is therefore important that You read this before You sign the declaration as any inaccuracies or omissions could affect the extent of cover provided or could invalidate Your insurance protection.

Material Circumstances

Please remember that you must make a fair presentation of the risk to us. This means that you must:

(1) disclose to us every material circumstance which you know or ought to know or, failing that, sufficient information to alert us that we need to make further enquiries; and

(2) make such disclosure in a reasonably clear and accessible manner; and

(3) ensure that, in such disclosure, any material representation as to a: (a) matter of fact is substantially correct; and (b) matter of expectation or belief is made in good faith.

A material circumstance is one that is likely to influence an insurer in the acceptance and assessment of the application. You must also make a fair presentation to us in connection with any variations, e.g. changes you wish to make to your policy. If you fail to make a fair presentation of the risk then this could affect the extent of cover provided or could invalidate your policy, so if you are in any doubt as to whether a circumstance is material then it should be disclosed to us.

Disclosures should be specific and made in a reasonably clear and accessible manner. We will not be deemed to have knowledge of any information generally referred to (for example the contents of company websites listed in the risk presentation) or any matter not expressly drawn to our attention.

Each renewal invitation is made on the basis of the information we have at the time it is issued. We may revise or withdraw it if, before the date your renewal takes effect, any event occurs that gives rise to a claim or alters the material circumstances under this insurance, even if we are notified after your renewal date.

A specimen copy of the policy wording is available on request. You should keep a record (including copies of letters) of all information supplied to us for the purposes of the renewal of this insurance. A copy of the completed application will be supplied on request within a period of three months after its completion.

Data Protection – Privacy Notice

Personal Information

Aviva Insurance Limited is the main company responsible for your Personal Information (known as the controller).

We collect and use Personal Information about you in relation to our products and services. Personal Information means any information relating to you or another living individual who is identifiable by us. The type of Personal Information we collect and use will depend on our relationship with you and may include more general information (e.g. your name, date of birth, contact details) or more sensitive information (e.g. details of your health or criminal convictions).

Some of the Personal Information we use may be provided to us by a third party. This may include information already held about you within the Aviva group, information we obtain from publicly available records, third parties and from industry databases, including fraud prevention agencies and databases.

This notice explains the most important aspects of how we use your Personal Information, but you can get more information by viewing our full privacy policy at aviva.co.uk/privacypolicy or requesting a copy by writing to us at: The Data Protection Team, Aviva, PO Box 7684, Pitheavlis, Perth PH2 1JR. If you are providing Personal Information about another person you should show them this notice.

Personal information we collect and how we use it

We will use personal information for a number of purposes including providing our products and services and fraud prevention.

We also use profiling and other data analysis to understand our customers better, e.g. what kind of content or products would be of most interest, and to predict the likelihood of certain events arising, e.g. to assess insurance risk or the likelihood of fraud.

We may carry out automated decision making to decide on what terms we can provide products and services, deal with claims and carry out fraud checks. More information about this, including your right to request that certain automated decisions we make have human involvement, can be found in the “Automated Decision Making” section of our full privacy policy.

We may process information from a credit reference agency, including a quotation search where you are offered an Aviva credit payment facility. More information about this can be found in the “Credit Reference Agencies” section of our full privacy policy.

We may use Personal Information we hold about you across the Aviva group for marketing purposes, including sending marketing communications in accordance with your preferences. If you wish to amend your marketing preferences please contact us at: contactus@aviva.com or by writing to us at: Aviva, Freepost, Mailing Exclusion Team, Unit 5, Wanlip Road Ind Est, Syston, Leicester, LE7 1PD. More information about this can be found in the “Marketing” section of our full privacy policy.

Your Personal Information may be shared with other Aviva group companies and third parties (including our suppliers such as those who provide claims services and regulatory and law enforcement bodies). We may transfer your Personal Information to countries outside of the UK but will always ensure appropriate safeguards are in place when doing so.

You have certain data rights in relation to your Personal Information, including a right to access Personal Information, a right to correct inaccurate Personal Information and a right to erase or suspend our use of your Personal Information. These rights may also include a right to transfer your Personal Information to another organisation, a right to object to our use of your Personal Information, a right to withdraw consent and a right to complain to the data protection regulator. These rights may only apply in certain circumstances and are subject to certain exemptions. You can find out more about these rights in the "Data Rights" section of our full privacy policy or by contacting us at dataprt@aviva.com

Marketing

We also use personal information we hold about you across the Aviva Group to help us identify and tailor products and services that may be of interest to you. We will only communicate with you in accordance with any marketing preferences you have provided to us. We will continue to do this after your policy has ended.

If you wish to amend your marketing preferences, change how you would like us to communicate with you or tell us to stop marketing to you, you can do so in the following ways:

- Contact us by:
  - phone: 01603 622200 or +44 1603 604999 (from abroad)
  - email: helpdesk@aviva.co.uk
  - post: Aviva, Freepost, Mailing Exclusion Team, Unit 5, Wanlip Road Ind Est, Syston, Leicester, LE7 1PD

How long we keep your personal information for

We maintain a retention policy to ensure we only keep personal information for as long as we reasonably need it for the purposes explained in this notice. We need to keep information for the period necessary to administer your insurance and deal with claims and queries on your policy. We may also need to keep information after our relationship with you has ended, for example to ensure we have an accurate record in the event of any complaints or challenges, carry out relevant fraud checks, or where we are required to do so for legal, regulatory or tax purposes. We will also use this information for marketing purposes.

Your rights

You have various rights in relation to your personal information, including the right to request access to your personal information, correct any mistakes on our records, erase or restrict records where they are no longer required, object to use of personal information based on legitimate business interests, including profiling and marketing, ask not to be subject to automated decision making if the decision produces legal or other significant effects on you, and data portability.

For more details in relation to your rights, including how to exercise them, please see our full privacy policy or contact us - refer to the "Contacting us" details below.

Contacting us

If you have any questions about how we use personal information, or if you want to exercise your rights stated above, please contact our Data Protection team by either emailing them at dataprt@aviva.com or writing to the Data Protection Officer, Level 5, Pitheavlis, Perth PH2 0NH.

If you have a complaint or concern about how we use your personal information, please contact us in the first instance and we will attempt to resolve the issue as soon as possible. You also have the right to lodge a complaint with the Information Commissioners Office at any time.

Fraud Prevention and Detection

In order to prevent and detect fraud we may at any time:

- Share information about you with other organisations and public bodies including the Police;
- Undertake credit searches and additional fraud searches;
- Check and/or file your details with fraud prevention agencies and databases, and if you give us false or inaccurate information and we suspect fraud, we will record this to prevent fraud and money laundering.

We and other organisations may also search these agencies and databases to:

- Help make decisions about the provision and administration of insurance, credit and related services for you and members of your household;
- Trace debtors or beneficiaries, recover debt, prevent fraud and to manage your accounts or insurance policies;
- Check your identity to prevent money laundering, unless you provide us with other satisfactory proof of identity;
- Check details of job applicants and employees.

Claims History

- Under the conditions of your policy you must tell us about any insurance related incidents (such as fire, water damage, theft or an accident) whether or not they give rise to a claim. When you tell us about an incident we will pass information relating to it to a database.
- We may search these databases when you apply for insurance, in the event of any incident or claim, or at time of renewal to validate your claims history or that of any other person or property likely to be involved in the policy or claim.

You should show these notices to anyone who has an interest in the insurance under the policy.

Choice of Law

The appropriate law as set out below will apply unless you and the insurer agree otherwise:

- The law applying in that part of the UK, the Channel Islands or the Isle of Man in which you normally live or (if applicable) the first named policyholder normally lives, or
- In the case of a business, the law applying in that part of the UK, the Channel Islands or the Isle of Man where it has its principal place of business, or
- Should neither of the above be applicable, the law of England and Wales will apply.

If You Have a Complaint

If for any reason you are unhappy with the product or service, please get in touch as soon as possible. For contact details and more information about the complaints procedure please refer to your policy documents. Where a complaint cannot be resolved to your satisfaction you may be able to ask the Financial Ombudsman Service (FOS) to carry out an independent review. Whilst firms are bound by their decision you are not. Contacting them will not affect your legal rights. You can contact the FOS on 0800 023 4567 or visit their website at www.financial-ombudsman.org.uk, where you will find further information

Telephone Call Recording

For our joint protection telephone calls may be recorded and/or monitored.