



Association of British Insurers



Insurance
Fraud
Bureau



Helping to Reduce Insurance Fraud when Customers
Apply for Products

A Good Practice Guide

October 2011

Foreword

Insurance is a unique form of contracting based on mutual trust between insurers and customers. The vast majority of customers do not abuse that trust. However, some do, and incur costs for the industry which are ultimately borne by honest customers. Regrettably there will always be people who will abuse that trust. The industry should take steps to protect the vast majority of customers who are honest from the unscrupulous few.

In 2008 the ABI estimated that undetected general insurance fraud cost insurers £1.9bn. This adds £44 a year to the average cost of each policyholder.

Much effort has been successfully invested by the insurance industry to detect insurance fraudsters, particularly when claims are being made. The Insurance Fraud Bureau is very successful at detecting organised fraudsters which may otherwise have gone undetected by individual insurers.

While the fight against fraudulent insurance claims must continue, it is also important that the industry takes an holistic view to combating fraud risk by seeking to detect fraud throughout the lifetime of a policy, including during the policy application and inception process.

There are significant benefits for the insurance industry in extending fraud controls to the application stage of the insurance buying process. The insurance industry will be better able to protect itself against payment fraud, ensure their customers premiums are correctly rated and of course intercept potential fraud before it becomes a problem.

By addressing fraud at an early stage, brokers and comparison websites may benefit in having a better performing portfolio of customers to present to insurers, thereby creating the potential to secure preferential terms from insurers.

This guidance seeks to summarise known industry good practices used to detect fraudsters when they apply for products. There is no one-size-fits-all solution as each insurer, broker and comparison website has their own unique business model.

Contents

1. Introduction
2. Identity and address of the customer
3. Is the customer a known fraudster?
4. Misrepresentations
5. Manipulation of risk information
6. Illegal or “ghost” insurance advisers
7. Backdating of cover
8. Payment of premium
9. Customer education
10. Market and own intelligence
11. Other developments and issues

1. Introduction

- **The purpose of the guidance**

The guidance sets out a series of high-level standards insurers, brokers and comparison websites may wish to adopt to help to reduce their exposure to fraud when customers apply for products.

- **The status of the guidance**

This is not FSA-confirmed industry guidance¹. This is a voluntary good practice guide for insurers, brokers and comparison websites.

- **Authors**

- Association of British Insurers
- British Insurance Brokers' Association
- Institute of Insurance Brokers
- Insurance Fraud Bureau
- Moneysupermarket.com
- Comparethemarket.com
- Gocompare.com
- Confused.com

- **Implementation**

This guidance is available to all insurers, brokers and insurance comparison websites from October 2011.

- **Review and update**

While the guidance is voluntary, all insurers, brokers and insurance comparison websites are encouraged to identify new industry practices which may be added to the guidance to help reduce the amount of insurance fraud perpetrated. New issues may be incorporated into the guidance following consultation with and agreement of the authors.

- **Definition of application fraud**

Where a policyholder, applicant or intermediary either:

- a) Deliberately and dishonestly misrepresents/fails to disclose material facts, when asked, at or before policy inception, amendment or renewal that would materially impact either the policy terms and conditions, the level of premium required or the acceptance of the policy issue/renewal for financial gain; or
- b) Fraudulently uses or manipulates credit or charge cards, bank direct debit mandates or other means to avoid payment of policy premium; or

¹ "FSA confirmed industry guidance" is industry guidance that has been formally confirmed by the FSA as helping users meet the FSA's regulatory requirements.

- c) Manipulates the policy set up/application/payment cycle to fraudulently obtain premium refunds from the insurer; or
- d) Forges or otherwise falsifies certificates of insurance or other insurance documents to obtain further documentation, or otherwise misrepresents cover or their identity to third parties; or
- e) Deliberately incepts a policy with the intent to claim (pre-meditated fraud) – either for a genuine event which occurred prior to inception of the policy or with the intention to make a false claim. This could include a risk of an organised fraud attack; or
- f) Is an illegal or “Ghost” insurance adviser, sometimes wrongly referred to as 'ghost brokers' who are not authorised by the Financial Services Authority or the Financial Conduct Authority. They prey on vulnerable groups of customers who find it difficult for language or risk reasons to access insurance products, usually motor insurance as it is a legal requirement. The illegal or “ghost” insurance advisers charge a fee to the customer to source their insurance and then usually misrepresent the customer’s risk information to secure an acceptable level of premium or fail to take out a policy and provide the ‘policyholder’ with false insurance documents. Some customers are unwitting victims of this fraud. Ghost insurance advisers often use false, fraudulent or stolen payment details to purchase the policies.

2. Identity and address of the customer - Is the customer who they say they are?

The following are some examples of good practices used in the industry that firms may wish to consider using.

Know Your Customer - Investment products are generally subject to Know Your Customer (KYC) requirements requiring customers to verify that they are who they say they are and they live at the address supplied in addition to verifying the source of funds to satisfy anti-money laundering legislation and rules. However, suppliers of general insurance products are not required to carry out the same level of checks but firms may wish to consider undertaking these types of checks.

- Electoral Register – Check the abbreviated electoral register. This may be done directly or via a specialist provider.
- Post Office (PO) box addresses – Consider why a P.O. box is being used. Can the reason be justified? Request and verify the actual address of the customer if you are unsure.
- Royal Mail - Monitor returned mail marked “gone-away” and “not known at this address” as these may be indicators of possible fraud. Even if premiums are being paid the insurance contract may be a feeder document to establish a bogus identity to be used for more serious crime.
- Commercial database providers – Consider using one of the commercially available databases to verify addresses.
- National Insurance (NI) number – When the NI number is requested, check that it is in the format of UK National Insurance numbers.
- Payment validation – see paragraph 8.

Passport Validation Service (PVS) – The service allows accredited organisations to verify information on a passport against the Home Office [Identity and Passport Service's](#) (IPS's) Passport database to check its authenticity.

- Postal address and risk address – Check that there is a good reason for differences between the postal address and risk address.

3. Is the customer a known fraudster?

What is available to firms to help them identify whether the customer has committed fraud before?

- Consider using commercially available databases of known fraudsters.

- The ABI and the Insurance Fraud Bureau is to launch the industry's own Insurance Fraud Register of known insurance fraudsters in 2012.

4. **Misrepresentation of rating factors**

Premiums are frequently based on several variable rating factors. The industry relies on the facts being represented correctly by customers, so what can be done to check whether rating factors are being manipulated to create a more favourable picture.

- Manipulation of risk factors and material facts - Firms should be alive to the potential within their systems and controls for customers to manipulate risk factors to achieve better terms and conditions. Firms should take measures to validate significant factors.
- Monitoring trends in rating factors - Identifying new and unusual trends in rating factors may indicate fraudulent activity requiring further investigation. For example all customers from a source of business garaging their cars to achieve better premiums.
- Validation of representations and rating factors – Detecting fraud at the application stage relies on the validation of representations made by customers. The greater the level of validation adopted, the greater will be the chances of detecting misrepresentations. The following are some examples of validations currently adopted by the industry. Each firm has a different profile of customers and risk which may require different and innovative methods of validation to address the risk. Validation does not have to be restricted to the application process. It may be prudent to include validation systems at all stages of the lifecycle of policies for pre-sale, post-sale, renewal and when claims are made.
- No Claims Discount (motor insurance) - Customers are usually required to provide proof of entitlement to a new insurer. It is easy to forge a proof so firms may wish to verify the authenticity of the proof with the rescinding insurer. Firms may wish to check against records held by the Claims and Underwriting Exchange (CUE). The verification of overseas proof of NCD poses a significant challenge to UK insurers.
- Motor Insurance “Fronting” – That is, another person, often a parent or other relative, is nefariously identified as the main user to obtain a lower premium. Some firms use a score card of indicators such as the order of listing of drivers or the mismatch of main user and premium payments to trigger further investigation.
- Claims history. If in doubt, verify against the Claims and Underwriting Exchange (CUE) or check with the previous insurer.

- Broker reporting mandates. When an insurance broker is authorised by a commercial insured to obtain quotes on the insured's behalf in addition to the insured's existing appointed insurance broker the ABI and BIBA has agreed voluntary guidance which may be adopted by all parties. The guidance clarifies how the new reporting broker may obtain confirmed claims experience in a standard format, subject to the insurer being satisfied that the new broker has obtained the appropriate authority from the insured. The existing insurer's confirmed claims experience is a reliable summary of the insured's claims experience and helps to avoid misrepresentations. The guidance may be viewed on the websites of [BIBA](#) and the [ABI](#).
- Vehicle annual mileage . Some insurers monitor the profile of vehicle mileages for customers of intermediaries to identify unusual patterns of consistently low mileages used to fraudulently obtain lower premiums.
- Motor insurance – use of vehicle – Cross check the occupation with the use of the vehicle e.g. occupation stated as retired but business use for courier/fast-food delivery etc.
- Occupation - Cross check changes of occupation at the application stage to identify if the changes vary dramatically, particularly if the final occupation selected is the lowest risk. Occupation is often used as a rating factor so it is important that customers select an occupation to best reflect what they actually do. However, it is sometimes difficult for customers to select from a limited list and may even deter honest applicants who wish to be accurate and they are unable to find a close match. However, some applicants deliberately select low risk occupations, having little or no relevance to their real occupation to manipulate a lower premium, which is clearly fraud.
- Motoring Convictions – Motoring convictions are frequently misrepresented. At the time of going to print, the ABI is working with DVLA to establish automatic verification of customers' licence and conviction information against DVLA records.
- Driving Licences - Customers may be required to provide a copy of their driving licence to a new insurer. Firms may wish to check that the correct licence is held in relation to the vehicle proposed, that it is current, any convictions shown match those disclosed, address shown matches the proposed address, and in the case of motorcycle insurance that a valid CBT certificate is held if required to support the driving licence.
- Postcode manipulation – Customers sometimes use valid postcodes that are in lower rated areas than their actual postcode to obtain cover at a lower premium. For example, West Scotland may be used rather than Central London as customers do not need a physical motor insurance certificate to be delivered to an address as long as they are registered on the Motor Insurance Database. Delivery of documents to the incorrect address should be an alert to an insurer, e.g. 'not known at this address' returns should be investigated.

- Does the policyholder / named driver exist? – Customers may create bogus individuals or bogus relationships to reduce their risk profile to obtain a lower motor insurance premium. This may lead to additional problems such as the insurer voiding contracts for non-existent policyholders. Firms may wish to adopt identity checks to identify anomalies.
- Common sense check – Firms should encourage staff to challenge and further investigate unusual or implausible scenarios which may be concocted by fraudulent customers. If it looks odd, it probably is.

5. Manipulation of risk information on web applications to obtain lower premiums

- Track multiple changes of risk information that should be relatively consistent during the pre-quote process, such as dates of birth, whether a vehicle is garaged and who will be the main driver. Some changes are of course expected such as the effect of changing a policy excess. Firms may wish to consider limiting the number of changes which can be made to key data fields which determine risk and premium.

6. Illegal or “ghost” insurance advisers

- To help identify the activity of “ghost” insurance advisers, firms should monitor their direct business to identify repeat sources of business such as e-mail addresses, mobile phone numbers, internet provider addresses and postal addresses. Firms may wish to consider limiting the number of applications or quotes allowed from the same source unless the intermediary has a valid agency with the insurer.

7. Backdating of cover

Backdating of cover is almost certainly fraudulent. So what can firms do to identify backdating of cover.

- Firms should monitor the quality of work of their cover issuers and audit them periodically.
- Firms should have systems and controls to identify irregularities in the sequence of dates on cover notes and challenge the issuer for a reason why.
- Some firms have withdrawn “cover-note” facilities from their agents to reduce the risk of them being misused.

8. Payment of premium – avoiding payment defaults

- Verify bank account details – Specialist commercial providers are able to verify that the bank account details are correct by checking for a valid match between the name of the bank, the sort code and the account holder's name. Verification helps to avoid fraudulent direct debit being set up.
- Deposit premiums - To avoid providing cover without having adequate premium, collect sufficient premium as a deposit to cover the period on-risk up to when the default would become apparent. Avoid providing cover without a deposit premium.
- Internet Provider (IP) address - Check for IP addresses that have been used previously for fraudulent purposes and for multiple use of the same address for different customers.
- County Court Judgements (CCJs) – Check if customers have a record of unsatisfied CCJs as this may provide an indication of future behaviours, e.g. identifies a propensity to default on payments.
- Recovery of motor insurance certificates - To avoid incurring Road Traffic Act(RTA) liability it is important to recover motor insurance certificates issued within the inception cancellation period (cooling-off period) required by FSA rules or at any other point during the life of the policy to avoid continuing liability under the RTA for those in possession of a motor insurance certificate. Refer to Section 147 of the RTA for details about the recovery of motor insurance certificates including the surrender of electronic certificates.
- Payment by credit card not present.- To identify whether customers are using a an inappropriate credit card, firms should comply with PCI Data Security Standards – e.g. by collecting CV2 or 3D secure verification on card transactions to avoid Card Not Present fraud.
- Credit ratings – When providing credit to customers, firms should check the customer's credit rating to help identify potential risk of default. Permission must first be sought from the customer. Several commercial databases are available to firms.

9. Customer education and warnings

- Ensure your sales process clearly and unambiguously explains what insurance fraud is and warns customers of the serious consequences of committing insurance fraud. Clarity about what insurance fraud is and the consequences of committing it helps to deter potential fraudsters at the point of application and for future applications for insurance.

- Firms should use any opportunity when communicating about fraud to stress the seriousness of the offence and that fraudulent customers may be prosecuted and may even face a custodial sentence. Stress that insurance fraud is recorded and may make financial services harder to access in future.

10. Market and own Intelligence

- There are several sources of market intelligence available to the industry to help identify fraudulent insurance applications including:
 - ↳ The Insurance Fraud Bureau (IFB) which issues intelligence alerts.
 - ↳ The Insurance Fraud Investigators Group (IFIG) issues e-alerts to their members and forum topics of new typologies etc.
 - ↳ Serious Organised Crime Agency (SOCA) issue alerts to the industry directly and via trade associations and other industry bodies.
 - ↳ Commercial providers also supply useful intelligence from other sectors outside the insurance industry.
- Use your firms own intelligence. You may provide several products to the same customer. Sharing information within an organisation is valuable intelligence and may prevent another area of your firm from making a costly mistake.

11. Other developments and issues

- DVLA verification – The ABI and BIBA are working with DVLA to establish automatic verification of customers' licence and conviction information by insurers against DVLA records.
- NCD database – The ABI is currently giving consideration to the creation of a database of NCD entitlement.
- The Insurance Fraud Register – The ABI and the Insurance Fraud Bureau (IFB) are to establish the register of proven insurance fraudsters in 2012.
- Don't forget to promote the IFB Cheatline on 0800 422 0421 and online at www.insurancefraudbureau.org/report/
- Firms must always comply with current legal requirements, including data protection and competition laws.