



Insurance
Fraud
Bureau

Membership Rules and Governance Manual

1.0

APRIL 2025

Contents

1. INTRODUCTION	7		
1.1. Introduction	8		
1.1.1. Enabling you to make informed decisions	8		
1.1.2. Creating a positive impact for society	8		
1.1.3. Delivering through trusted partnerships	8		
1.1.4. Data protection	8		
1.2. Using This Document	9		
1.2.1. Approach to Rules and Governance	9		
1.3. IFB Data	10		
1.3.1. Industry Transactional Data	10		
1.3.2. Suspect Data	10		
1.3.3. Confirmed Fraud Data	10		
1.4. IFB Intelligence Sharing	11		
1.5. Permitted Purpose	11		
1.5.1. Permitted Purpose of Use for IFB Data	11		
1.6. Understanding this Document	11		
1.6.1. The Membership Rules and Governance Manual	11		
1.6.3. Explanation of Tables and Key	16		
2. ROLES AND RESPONSIBILITIES	17		
2.1. Roles and Responsibilities	18		
2.1.1. Applicable Roles and Responsibilities	18		
2.2. Head of Fraud, Interface Manager and Users	19		
2.2.1. Requirement	19		
2.2.2. Guiding Principle	19		
2.2.3. Authorised Users Must:	19		
2.2.4. Interface Managers Must:	19		
2.2.5. Interface Managers May:	20		
2.2.6. Interface Managers Must Not:	20		
2.2.7. Heads of Fraud Must:	20		
2.2.8. Governance	20		
3. SEARCH	21		
3.1. Ensuring Lawful and Compliant Search Activity	22		
3.2. Search – ‘Reasonable Grounds’	23		
3.2.1. Ensuring Lawful and Compliant Search Activity	23		
3.2.2. Requirement	23		
3.2.3. Guiding Principle	23		
3.2.4. Authorised Users Must:	23		
3.2.5. Authorised Users Must Not:	24		
3.2.6. Interface Managers Must:	24		
3.2.7. Interface Managers Must Not:	24		
3.2.8. Governance	24		
4. GENERIC DATA FEED	25		
4.1. Generic Data Feed	26		
4.1.1. Ensuring Integrity of the Bulk Intelligence Data	26		
4.2. Generic Data Feed	27		
4.2.1. Requirement	27		
4.2.2. Guiding Principle	27		
4.2.3. Authorised Users Must:	27		
4.2.4. Authorised Users May:	27		
4.2.5. Authorised Users Must Not:	27		
4.2.6. Interface Managers Must:	27		
4.2.7. Interface Managers Must Not:	27		
4.2.8. Interface Managers Should:	28		
4.2.9. Governance	28		
5. CONFIRMED FRAUD DATA	29		
5.1. Confirmed Fraud Data	30		
5.1.1. Ensuring Appropriate Use of the Confirmed Fraud Data	30		
5.2. Confirmed Fraud Data	31		
5.2.1. Ensuring Appropriate Use of the Confirmed Fraud Data	31		
5.2.2. Requirement	31		
5.2.3. Guiding Principle	31		
5.2.4. Authorised Users Must:	31		
5.2.5. Authorised Users Must Not:	31		
5.2.6. Interface Managers Must:	32		
5.2.7. Interface Managers Must Not:	32		
5.2.8. Interface Managers May:	32		
5.2.9. Governance	32		



CONTENTS

6. AUTOMATED DECISION MAKING	33
6.1. Automated Decision Making	34
6.1.1. Use of Automated Decision Making Against Confirmed Fraud Data	34
6.2. Automated Decision Making	35
6.2.1. Use of Automated Decision Making Against Confirmed Fraud Data	35
6.2.2. Requirement	35
6.2.3. Principle	35
6.2.4. Heads of Fraud and Interface Managers Must:	35
6.2.5. Heads of Fraud and Interface Managers Must Not:	36
6.3. Automated Decision Making	37
6.3.1. Use of Automated Decision Making Against Confirmed Fraud Data	37
6.3.2. Governance	38

7. DATA DISCLOSURE	39
7.1. Data Disclosure	40
7.1.1. Ensuring Compliant Onward Data Disclosure	40
7.2. Data Disclosure	41
7.2.1. Requirement	41
7.2.2. Guiding Principle	41
7.2.3. Authorised Users Must:	41
7.2.4. Authorised Users May:	41
7.2.5. Authorised Users Must Not:	41
7.2.6. Interface Managers May:	42
7.2.7. Interface Managers Must:	42
7.2.8. Interface Managers Must Not:	42
7.2.9. Governance	42

8. ENSURING RECIPROCITY	43
8.1. Ensuring Reciprocity	44
8.1.1. Ensuring Fair and Proportional Contribution	44
8.2. Ensuring Reciprocity	45
8.2.1. Requirement	45
8.2.2. Guiding Principle	45
8.2.3. Heads of Fraud Must:	45

8.2.4. Heads of Fraud Should:	45
8.2.5. Interface Managers Must:	45
8.2.6. Interface Managers Should:	45
8.2.7. Interface Managers Must Not:	46
8.2.8. Interface Managers May:	46
8.2.9. Authorised Users Should:	46
8.2.10. Authorised Users Should Not:	46
8.2.11. Governance	46

9. LOADING – THRESHOLDS 47

9.1. Loading – Thresholds	48
9.1.1. Ensuring the Integrity of Data Loaded	48
9.2. Loading – Thresholds	49
9.2.1. Requirement	49
9.2.2. Guiding Principle	49
9.2.3. Authorised Users Must:	49
9.2.4. Authorised Users Must:	49
9.2.5. Authorised Users May:	49
9.2.6. Authorised Users Must Not:	49
9.2.7. Interface Managers Must:	50
9.2.8. Interface Managers Must Not:	50
9.2.9. Governance	50

10. LOADING – TRANSPARENCY 51

10.1. Loading – Transparency	52
10.1.1. Ensuring Appropriate Transparency Towards Data Subjects	52
10.2. Loading – Transparency	53
10.2.1. Requirement	53
10.2.2. Guiding Principle	53
10.2.3. Authorised Users Must:	53
10.2.4. Authorised Users Should:	53
10.2.5. Authorised Users Must Not:	53
10.2.6. Heads of Fraud Must:	53
10.2.7. Interface Managers Must Not:	53
10.2.8. Governance	53



CONTENTS

11. LOADING – ACCURACY	54		
11.1. Loading – Accuracy	55		
11.1.1. Maintaining the Accuracy and Relevancy of Data Loaded	55		
11.2. Loading – Accuracy	56		
11.2.1. Requirement	56		
11.2.2. Guiding Principle	56		
11.2.3. Authorised Users Must:	56		
11.2.4. Authorised Users Must Not:	56		
11.2.5. Interface Managers Must:	56		
11.2.6. Interface Managers Must Not:	56		
11.2.7. Governance	57		
12. COMPLAINTS AND DSARS	58		
12.1. Complaints and DSARs	59		
12.1.1. Safeguarding Data Subject Rights	59		
12.2. Complaints and DSARs	60		
12.2.1. The IFB Complaints Policy	60		
12.2.2. Requirement	60		
12.2.3. Guiding Principle	60		
12.2.4. Authorised Users Must:	60		
12.2.5. Interface Managers Must:	60		
12.2.6. Interface Managers Must:	61		
12.2.7. Interface Managers Must Not:	61		
12.2.8. Interface Managers Must:	61		
12.2.9. Interface Managers Must Not:	61		
12.2.10. Governance	62		
13. DATA INTEGRITY	63		
13.1. Data Integrity	64		
13.1.1. Ensuring Highest Standards of Data Protection and Information Security	64		
13.2. Data Integrity	65		
13.2.1. Requirement	65		
13.2.2. Guiding Principle	65		
13.2.3. Authorised Users Must:	65		
13.2.4. Authorised Users Must Not:	65		
13.2.5. Interface Managers Must:	66		
13.2.6. Interface Managers Must Not:	66		
13.2.7. Interface Managers Should:	66		
13.2.8. Governance	67		
14. TRAINING AND COMPLIANCE	68		
14.1. Training and compliance	69		
14.1.1. Ensuring User Awareness and Good Governance	69		
14.2. Training and compliance	70		
14.2.1. Requirement	70		
14.2.2. Guiding Principle	70		
14.2.3. Authorised Users Must:	70		
14.2.4. Authorised Users Should:	70		
14.2.5. Authorised Users Must Not:	70		
14.2.6. Interface Managers Must:	70		
14.2.7. Interface Managers Must Not:	71		
14.2.8. Interface Managers Should:	71		
14.2.9. Interface Managers May:	71		
14.2.10. Governance	71		
15. MANAGEMENT INFORMATION	72		
15.1. Management Information	73		
15.1.1. Leveraging MI for Benefits Mapping and Evidencing Compliance	73		
15.2. Management Information	74		
15.2.1. Requirement	74		
15.2.2. Guiding Principle	74		
15.2.3. Interface Managers Must:	74		
15.2.4. Interface Managers Should:	74		
15.2.5. Interface Managers Must Not:	74		
15.2.6. Governance	74		



CONTENTS

16. COMPLIANCE SUPPORT FRAMEWORK 75

16.1. Compliance Support Framework	76
16.1.1. Ensuring Member Adherence through Compliance Support	76
16.2. Compliance Support Framework	77
16.2.1. Requirement	77
16.2.2. Guiding Principle	77
16.2.3. Authorised Users Must:	77
16.2.4. Interface Managers and Heads of Fraud Must:	77
16.2.5. Interface Managers and Heads of Fraud Must Not:	77
16.2.6. Governance	77
16.2.7. Introduction	78
16.2.8. How the framework operates	78
16.2.9. Event Support and Measures Risk Scoring Matrix	78
16.3. Quarterly Compliance Score Matrix	81
16.3.1. How the Quarterly Compliance Score is calculated	81

17. APPENDIX 83

17.1. Fraud Definitions	84
17.1.1. Confirmed Fraud Definition	84
17.1.2. Provided that...	84
17.2. Data Retention	85
17.2.1. IFB Data-Retention Periods	85
17.3. National Intelligence Model (NIM) Grading	86
17.3.1. Source Evaluation	86
17.3.2. Intelligence Reliability	87
17.3.3. Intelligence Confidence Matrix	88
17.3.4. Handling Codes	88
17.3.5. Action and Sanitisation Codes	89
17.3.6. Crime Levels	89
17.4. IFB Complaints Policy	90
17.4.1. Responsibilities	90
17.4.2. Introduction	90
17.4.3. How is a complaint defined?	90
17.4.4. Receiving the complaint	90
17.4.5. Service Level	91
17.4.6. Who should investigate and respond to complaints relating to Data loaded to the system?	91
17.4.7. Complaints attracting media attention or public interest	91
17.4.8. High-profile complaints	91
17.4.9. Insurer complaints process	92
17.5. IFB Complaints Policy	92
17.5.1. Acknowledgment of the complaint	92
17.5.2. Investigation	93
17.5.3. Removal of Records	93
17.5.4. Management Information	93



DOCUMENT CONTROL

Purpose and Control

Category	Comments		
Status	ISSUED		
Issued:	February 2025		
Document author:	IFB Service Delivery Manager		
Document owner:	IFB Director		
Purpose:	To provide Users with an outline of their obligations in respect of IFB Membership.		
Notice	This document is intended for general use and should not be considered without reference to the complete IFB Membership Agreement.		

Version	Date	Author	Notes
Status	February 2025	IFB Service Delivery Manager Intelligence and Investigations Manager	Version 1.0 issued in AGM pack



I.

Introduction

We are the Insurance Fraud Bureau (IFB), a not-for-profit company established in 2006 as a central data hub for the industry to share fraud and intelligence data.

We lead the collective fight against insurance fraud and serve as the industry's Data hub for comprehensive fraud intelligence and analytics. We'll help you protect your customers, reduce fraud-related costs and strengthen public trust in the insurance sector.



I. INTRODUCTION

I.1. INTRODUCTION

I.1.1. Enabling you to make informed decisions

With our unique breadth of industry Data, analytics and intelligence sharing, we help our Members, and the wider insurance industry, better understand their exposure to insurance fraud. This enables you to make effective and efficient decisions on suspected fraud cases.

I.1.2. Creating a positive impact for society

As a not for a not-for-profit organisation, every action we take is solely aimed at reducing insurance fraud, protecting the public and keeping costs down to help your customers.

I.1.3. Delivering through trusted partnerships

Our joined-up approach connecting our Members to each other and regulatory and law enforcement agencies, provides you with a thorough understanding of your exposure to emerging threats, helping you to protect your honest customers.

I.1.4. Data protection

As a data-driven Member organisation – accountable both to the insurance industry and the collective Data Subjects whose Data we are entrusted to hold – the IFB is fully committed to ensuring the highest standards of Data protection and integrity. As independent Data Controllers, the responsibility for the quality, protection, and lawful use of the Data submitted to and maintained on industry counter-fraud platforms is shared between the IFB and its Members. As such, each Member is liable for ensuring the accuracy of records loaded and searches are conducted appropriately and proportionately.



1. INTRODUCTION

1.2. USING THIS DOCUMENT

This guide outlines the essential controls, principles and standards necessary to protect Data held within IFB platforms, ensuring the highest standards of fairness and transparency in terms of how this sensitive Data must be handled.

As an IFB Member, your organisation must adhere to the guidelines set out in this document and demonstrate compliance. By following the guide and participating in our compliance processes, Members can maintain compliance with the IFB standards, while also fully harnessing the benefits of direct access to industry counter-fraud Data.

The Membership Rules and Governance Manual operates as a collaborative approach between Members and the IFB. Members will be clear about the actions they must take to ensure they are compliant with the Rules and any Measures that may be implemented as a consequence of non-compliance. IFB will support Members in the process and provide training and guidance as necessary to support compliance.

The aim of this approach is to not only support Members in gaining the most value from IFB services, but to promote collaboration between the wider Membership and IFB in supporting broader counter-fraud efforts. As a consequence, continued feedback on the Rules and Governance is invited to help drive continued improvements to the framework.

1.2.1. Approach to Rules and Governance

The Rules set out requirements Members Must / Must Not, Should / Should Not, May undertake.

The Governance model will take the following approach to these requirements:

- 1.2.1.1. **Must / Must Not** – Must / Must Not requirements must be strictly adhered to, and will be subject to some form of compliance checks, training and / or evidential requirement in order to demonstrate compliance. Failure to comply may lead to specific Measures, which must be undertaken by a Member to demonstrate subsequent compliance.
- 1.2.1.2. **Should / Should Not** – Should / Should Not items are not strict requirements; however, Members are recommended or expected to uphold them. Compliance with these items may include provision of compliance checks, training and / or evidence, but may also include broader conversations about how to best comply with them. The IFB will actively support Members to ensure that these requirements can be complied with.
- 1.2.1.3. **May** – Items listed as May represent processes which can be applied at Members' discretion, but may provide opportunities for better engagement across the Member base. The IFB will actively support Members to maximise the value of their membership and that of the wider Member base.



1. INTRODUCTION

1.3. IFB DATA

1.3.1. Industry Transactional Data

The industry Transactional Data held by the IFB consists of:

- 1.3.1.1. Navigate (formerly MID) Data, consisting of both personal and commercial motor policies.
- 1.3.1.2. CUE claims Data, made up of Data fed in from CUE Motor, CUE Property and CUE Personal Injury.
- 1.3.1.3. MIAFTR Data, consisting of lost, stolen and written-off vehicle Data.

Delta files from these source databases are ingested into the IFB's counter-fraud solution, which provides advanced network detection capabilities across motor, property and liability lines of business. It allows IFB Members to remotely access the industry's Transactional Data, focusing on at-risk entities and networks that potentially link to organised fraud and gain contextual insights as they emerge.

1.3.2. Suspect Data

The IFB makes available an industry-wide infrastructure, which enables the insurance industry to share intelligence on individuals, organisations and articles where there are reasonable grounds to believe that they are implicated in insurance fraud, via a single platform.

Pooling Suspect Data in one location will allow the insurance industry to consolidate intelligence on suspected insurance fraud, creating a more effective, efficient and secure model and 'single point of truth' for the industry and the IFB to process and disseminate intelligence. In turn, this will provide Users with the capability to raise requests for the IFB to perform intelligence development activities and provide feedback, as well as access information reports, intelligence products and investigations updates issued by the IFB.

1.3.3. Confirmed Fraud Data

The Confirmed Fraud register consists of the first industry-owned, cross-sector register of confirmed insurance fraudsters. The purpose of the register is to facilitate the sharing of Confirmed Fraud information with the aim of tackling volume fraud committed across the insurance industry.

The Confirmed Fraud register contains tens of thousands of records of proven fraud – both organised and opportunist – across all personal and commercial insurance product lines.

The Confirmed Fraud Data is also available to download in its entirety, enabling Members to wash this Data against their existing book of business and screen for potentially bad actors at source – subject to manual review and validation.



I. INTRODUCTION

I.4. IFB INTELLIGENCE SHARING

The IFB share intelligence with Members using the National Intelligence Model (NIM). Intelligence reports are produced using Data from the IFB Data, Member Data and intelligence provided by members of the public and law enforcement agencies.

IFB intelligence reports are issued in response to intelligence provided by Members, to share the details of proactive networks identified from the IFB Data, to share reports made to the Cheatline or to share intelligence provided by law enforcement. Intelligence reports are also shared with Members to provide updates on IFB investigations.

Where the IFB intends to develop a piece of intelligence to work towards some form of disruption, Members are requested to provide feedback on claims and policies identified in the report, or to provide new intelligence to support IFB investigations.

I.5. PERMITTED PURPOSE

I.5.1. Permitted Purpose of Use for IFB Data

‘Purpose’ means:

- I.5.1.1. the facilitation in a non-discriminatory manner only of the sharing of fraud-related information with the aim of reducing the amount of fraud committed across the insurance industry and therefore the cost of fraud across the insurance industry and the cost of such fraud to customers of the insurance industry;
- I.5.1.2. the prevention and / or detection and / or investigation of crime (including, the crime of insurance fraud);
- I.5.1.3. the apprehension and / or prosecution of offenders (including in respect of insurance fraud);
- I.5.1.4. the assessment or collection of any tax or duty or of any imposition of a similar nature;
 - I.5.1.4.1. the management of the risk of fraud by Members and the repudiation of insurance application and claims;
- I.5.1.5. the protection of insurers, other organisations within the insurance industry, and non-fraudulent insurance policy holders; and
- I.5.1.6. the facilitation of the consistent identification, classification, benchmarking, measurement and reporting of fraud across the insurance industry (including to the National Fraud Intelligence Bureau (NFIB), in a non-discriminatory manner only and in accordance with all applicable laws.

I.6. UNDERSTANDING THIS DOCUMENT

I.6.1. The Membership Rules and Governance Manual

Accountability – Members understand their roles and responsibilities to comply with the Rules and support reciprocity across the industry. The IFB will ensure there is meaningful feedback around the Governance processes to help support and improve member compliance. Any Measures applied will be clear and proportionate, and will reflect a collaborative approach of Members and the IFB working towards good governance.

Accessibility – The Governance framework will seek to be accessible to all members. All Governance documents will be accessible from a single location, be written in clear language and explain how they seek up uphold compliance with the Membership Rules. Regardless of size, product line or industry position, each Member will be subject to the same Governance model, which will seek to avoid resource-heavy or burdensome processes which may hinder engagement. Members will have easy access to Data regarding their interaction with IFB services and guidance provided about how to improve compliance.

Transparency – Any decision making regarding change to the framework or application of Measures will be open to oversight from Members. To support the collaborative cross-industry data-sharing approach, reporting of collective compliance should be made available alongside recommendations for improvements.



I. INTRODUCTION

I.6.2. Guide on Terminology Used

Member Type	Member Definition
Member – Insurer	Insurer Member of the IFB, as detailed in the Articles of Association.
Member – Non-Insurer	Refers to claims handling agents, loss adjusters, lawyers and investigators, or such other eligible parties as determined by the Board from time to time.
Community Member	A Member who may provide Data to the IFB but not directly receive Data.
Approved Third Party Member	Means those third parties approved by the IFB from time to time who are not Members but who are permitted access to the relevant Systems in accordance with terms equivalent to the terms of this agreement;

Role Type	Role Definition
Authorised User	Means those employees, agents, workers and independent contractors of the Member who are authorised by the Member to use the Systems.
Delegated User	Any Authorised User with additional responsibilities in respect of the Data, receives delegated tasking from the Interface Manager.
Interface Manager	Means the person appointed by the Member as the interface manager (or as any replacement or equivalent role required by the IFB from time to time), who shall be responsible for ensuring that the Member complies with the obligations in this agreement relating to the access to and use of the Systems, any data obtained from the Systems and any other IFB Materials;
Head of Fraud	Means the person appointed by the Member as the head of fraud (or as any replacement or equivalent role required by the IFB from time to time) for the purposes of this agreement, who shall be responsible for the day-to-day operation and management of this agreement for the Member and shall be the IFB's principle point of contact in respect of this agreement.



I. INTRODUCTION

I.6.2. Guide on Terminology Used

Glossary	Description
Board	Means the board of directors of IFB including the Executive Directors.
Business Day	Means a day, other than a Saturday, Sunday or public holiday, on which clearing banks are open for non-automated commercial business in the City of London.
Case	Refers to a Member's internal fraud investigation prior to loading.
Complaint	Has the meaning as captured under the UK Data Protection Act.
Confirmed Fraud Data	Means data (including personal data) relating to a person in circumstances where fraud is considered to have taken place, as further set out in Section 17.1 of this document.
Data	Refers to the IFB Data and Member Data (as defined in full in the Membership Agreement) in aggregate.
Data Breach	Means any accidental, unlawful or unauthorised destruction, loss, alteration, disclosure of, or access or damage to the Personal Data or any other unauthorised or unlawful processing of the Personal Data.
Data Protection	Has the meaning as set out in the Membership Agreement.
Data Subject	Has the meaning as captured under the UK Data Protection Act.
Data Subject Access Request (DSARs)	Means any requests from or on behalf of data subjects to exercise their rights under the Data Protection Legislation;
Fair Processing Notices	Means a fair processing notice which contains fair processing information as required by the applicable Data Protection Legislation (including but not limited to the requirements set out in Articles 13 and 14 of the UK GDPR).
Fraud Definition	Has the meanings as set out in Section 17.1 of this document.
Group	Has the meaning as set out in the Membership Agreement.
Intelligence Report	Means a report created by the IFB and which may be produced in combination with, or separately from, IFB Data, Member Data, data received by the IFB from third party partners with whom the IFB engages, and/or open source data obtained from publicly available sources, and such report shall be graded in accordance with NIM.



I. INTRODUCTION

I.6.2. Guide on Terminology Used

Glossary	Description
Member / Member organisation	Refers to the organisation that is signed up as a Member; inclusive of their Group, means a corporate body or entity involved in the Insurance Business, or belonging to a Group involved in the Insurance Business, or a Non-insurer involved in the Insurance Business, whose membership application to the IFB has been considered and approved by the Membership Committee and thereafter whose name is added as a Member on the register of members of IFB.
Membership Committee	Has the meaning as set out in the Articles of Association.
Membership Agreement (MSA)	Refers to the accompanying legal agreement signed between the Member and the IFB.
Membership Rules and Governance Manual	Refers to this document and means the membership rules and governance manual (including any operating rules) provided by the IFB to the Member from time to time.
NIM	Means the National Intelligence Model of the Home Office.
Non-Insurer	Means claims handling agents, loss adjusters, lawyers and investigators, or such other Applicant Member as determined by the Board from time to time who has entered into agreements with Members pursuant to which they assist those Members with certain elements of insurance claims, insurance fraud detection and investigation processes;
Personal Data	Means the personal data (as defined in the Data Protection Legislation) that is shared or made available by one party with or to the other party.
Record	Refers to the technical record loaded to the Database(s) as a result of a Case, as defined above.
Suspect Fraud Data	Data that has met the Suspect Fraud Definition as set out in 17.1 of this document.
System	Means any IT system, platform or database owned by, licensed to, operated by and/ or maintained by the IFB to which the Member has access as part of its membership and which is intended to assist in combating organised fraud in the UK insurance industry in connection with the Purpose.
Transactional Data	Refers to the CUE, MID and MIAFTR Data housed within the IFB Database.



I. INTRODUCTION

I.6.2. Guide on Terminology Used

Terminology	Description
Requirement	A short explanation to the functionality, product, output or compliance requirement in question.
Guiding Principle	The overarching principle governing User activity, to which all IFB staff and Members must subscribe.
Must	Mandatory or legal requirement that must be adhered to.
Must not	Prohibited action based on legal, contractual or regulatory requirement.
May	An action permitted and actionable by the Member at their discretion.
Measures	Action(s) required by a Member and / or IFB following a breach of a Rule, as detailed in Section 16 of this document
Should	A recommendation or expectation for a preferable or correct action.
Should not	A course of action not recommended or preferred, but not strictly prohibited.



I. INTRODUCTION

I.6.3. Explanation of Tables and Key

	1 Role or Member Type	2 Role or Member Type	3 Role or Member Type
Requirement	●	●	●
Requirement	●	●	●
Requirement	●	●	●

- Yes – Requirement applies to Users / Member type
- Partial – User plays supportive role in fulfilling requirement
- No – Requirement does not apply to this level of Users
- N/A – Requirement does not apply as Users / Member does not have access to the Data or service

Note: Colours assigned on table assume that successful due diligence to the Data has been completed by the Member.



2.

Roles and Responsibilities

Each Member must appoint a Head of Fraud and an Interface Manager to collectively ensure compliance with the Membership Rules and Membership Agreement. All Users must similarly adhere to these Rules and contribute towards a culture of Data protection, information security and collective Member compliance across the User base.

Users – whether junior or senior, IFB or Member – play a key role in ensuring the integrity, security and ethical usage of the shared Data, as well as in maintaining a collective culture of both awareness of and compliance with the IFB Membership Rules.



2. ROLES AND RESPONSIBILITIES

2.1. ROLES AND RESPONSIBILITIES

2.1.1. Applicable Roles and Responsibilities

- Yes
- Partial
- No
- N/A

	1 Heads of Fraud	2 Interface Manager	3 Authorised Users
Comply with Membership Rules and Membership Agreement	●	●	●
Adhere to National Intelligence Model (NIM)	●	●	●
Lead contact for a-to day operations and Member compliance	●	●	●
User / IP address admin	●	●	●
Audit / Compliance Check Responsibilities	●	●	●
Complaints and DSARs Responsibility	●	●	●
Legal and Contractual Responsibility	●	●	●
Report Data loss, misuse or Data Breach	●	●	●



2. ROLES AND RESPONSIBILITIES

2.2. HEAD OF FRAUD, INTERFACE MANAGER AND USERS

2.2.1. Requirement

Each Member **must** appoint a Head of Fraud and an Interface Manager to collectively ensure compliance with the Membership Rules and Membership Agreement. It is at the Member's discretion as to which individuals they nominate to the respective roles, provided they are a Member of the Fraud / Intelligence function, and / or represent designated counter-fraud personnel within the business, and are deemed of an appropriate level of seniority. Authorised Users (i.e., all Users other than and inclusive of those appointed to the above roles) **must** similarly adhere to these Rules and contribute towards a culture of Data protection, information security and collective Member compliance across the User base.

2.2.2. Guiding Principle

Users – whether junior or senior, IFB or Member – play a key role in ensuring the integrity, security and ethical usage of the shared Data, as well as in maintaining a collective culture of both awareness of and compliance with the Membership Rules and Membership Agreement.

2.2.3. Authorised Users Must:

- 2.2.3.1. Access and use IFB Data or System(s) only in accordance with the terms and conditions of the Membership Rules and Membership Agreement.
- 2.2.3.2. Ensure all personal login details to access IFB Data or System(s) are stored securely and are not shared with other Users or staff members
- 2.2.3.3. Search for and / or use Data only in accordance with the terms and conditions of the Membership Rules and Membership Agreement.
- 2.2.3.4. Undertake any e-learning training required by the IFB as a precondition of access to System(s) and the Data, and as otherwise required by the IFB.
- 2.2.3.5. Adhere in full to the National Intelligence Model (NIM) in terms of intelligence handling, which forms part of the IFB e-learning training package.
- 2.2.3.6. Ensure personal familiarity with and adherence to the Membership Rules (this document).
- 2.2.3.7. Immediately report any instances of actual, suspected or threatened unauthorised disclosure, misappropriation, misuse, loss, corruption, damage to, deletion of, or Data Breach in respect of any of the Data to their designated Interface Manager and Head of Fraud.
- 2.2.3.8. Treat the IFB published Contact Lists (containing details on Heads of Fraud, Interface Managers and Authorised Users) confidentially, only using

for the purpose of facilitating contact between fraud resource across organisations, and not for any other purposes.

2.2.4. Interface Managers Must:

In addition to the responsibilities set out above for Authorised Users, Interface Managers must:

- 2.2.4.1. Assume responsibility for day-to-day operational interactions with the IFB, including compliance with the Membership Rules and Membership Agreement.
- 2.2.4.2. Act as the principal point of contact in respect of day-to-day operations and matters relating to the Membership Rules and Membership Agreement.
- 2.2.4.3. Administrate User accounts on a day-to-day basis, advising the IFB in a timely manner of any required creation, deletion or amendment of User accounts.
- 2.2.4.4. Ensure no access to the Data (either directly or via bulk Data outputs) is provided to staff outside of the Member fraud or intelligence functions.
- 2.2.4.5. Ensure User training is completed in a timely manner, both on initial account creation and as otherwise required thereafter by the IFB.
- 2.2.4.6. Advise the IFB of any changes to the Member's IP address list, where updates are required.
- 2.2.4.7. Conduct various compliance checks and onsite audit activities of the Member's use of the services, as required from time to time by the IFB.
- 2.2.4.8. Handle complaints from Data Subjects in respect of Data Subject Access Requests (DSARs) and any breaches of the Data protection requirements.
- 2.2.4.9. Be aware that Interface Manager failure to fulfil these obligations could result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.
- 2.2.4.10. Report any instances of actual, suspected or threatened unauthorised disclosure, misappropriation, misuse, loss, corruption, damage to, deletion of, or Data Breach in respect of any of the Data to the IFB within 24 hours.
- 2.2.4.11. Inform the IFB of any changes of personnel in respect of the Interface Manager and Head of Fraud role. Please note this is a shared responsibility with Head of Fraud.



2. ROLES AND RESPONSIBILITIES

2.2.5. Interface Managers **May**:

- 2.2.5.1. Delegate responsibilities for the execution of certain functions (e.g. complaint handling, audit and compliance checks) to select Authorised Users within their Member organisation, which known as Delegated Users, on a day-to-day basis. However, the Interface Manager **retains overall responsibility and accountability** for ensuring these tasks are correctly executed, in line with the terms of the Membership Rules and Membership Agreement.

2.2.6. Interface Managers **Must Not**:

- 2.2.6.1. Ignore, delay or postpone any communications or actions in respect of IFB requirements in respect of the Membership Rules and Membership Agreement.
- 2.2.6.2. Fail to fulfil these obligations, as set out in the Membership Rules and Membership Agreement. **Failure to enact the aforementioned roles and responsibilities could result in formal escalation to the Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.**

2.2.7. Heads of Fraud **Must**:

In addition to the responsibilities set out above for Users, Heads of Fraud must:

- 2.2.7.1. Assume accountability for the exercise of the Member's rights and the performance of the Member's obligations under the Membership Rules and Membership Agreement.
- 2.2.7.2. Ensure that their Member organisation complies in full with the terms and conditions of the Membership Rules and Membership Agreement. This includes ensuring that the Member only accesses and uses IFB Data and System(s) in accordance with the terms and conditions of the Agreement.
- 2.2.7.3. Ensure that the Member appoints a primary Interface Manager and up to two suitable deputies (to be agreed with the IFB) to fulfil the duties and obligations of the Interface Manager (as set out above), in order to cover any periods of absence of the primary Interface Manager.
- 2.2.7.4. Ensure that any proposed variations to the Membership Rules and Membership Agreement are processed in a timely and accurate manner;

according to internal process and with any resultant queries being raised to the IFB within the three-month notice of variation window.

- 2.2.7.5. Act as escalation point in the event of Member dispute, Data Breach or failure of the Interface Manager to fulfil their obligations under the Membership Rules and Membership Agreement.
- 2.2.7.6. Inform the IFB of any changes of personnel in respect of the Interface Manager and Head of Fraud roles. Please note this is a shared responsibility with Interface Manager.

2.2.8. Governance

- 2.2.8.1. An acknowledgment of each role's responsibilities will be included in an annual attestation.
- 2.2.8.2. Authorised Users gaining access to the IFB Data and / or System(s) will be provided with compulsory training to ensure compliance with the Rules.
- 2.2.8.3. The IFB will provide Interface Managers with the details of Authorised Users accounts for review on a quarterly basis to ensure only appropriate Users have access to the IFB Data and / or System(s). Any inactive accounts will be automatically suspended.
- 2.2.8.4. Delegated Users must comply with any Rules associated with the responsibilities delegated to them.

Accountability – Each role will understand their responsibilities in ensuring the integrity, security and ethical usage of the IFB Data and / or System(s), supporting industry collaboration and ensuring compliance with the Membership Rules and Membership Agreement. The IFB and Interface Managers will work together to ensure Members' Authorised User lists remain accurate.

Accessibility – Training and supporting documentation will be readily accessible for all roles. Training material will use clear language, which will explain how each role can uphold their responsibilities and remain compliant with the Membership Rules and Membership Agreement.

Transparency – Members will understand the roles and responsibilities across the Membership. While the extent of training will differ across the Membership options, it will be consistent for each category to help build understanding across the Membership.



3.

Search

The IFB makes the industry Transactional, Suspect and Confirmed Fraud Data available to its Members to search against on a single-search basis, where a User has a pre-existing suspicion of fraud. Searches across the Data must only be used for the purposes of preventing, detecting and investigating fraud and complying with legal obligations.

The Data held by the IFB on the insurance industry's behalf includes Personal, Personal Sensitive and Special Category Data, which has added protections under GDPR. It is important that all Users treat this Data appropriately and sensitively. As such, searches conducted must be proportionate, legal, accountable and necessary, as well as premised on a 'reasonable grounds' to suspect fraud, in line with 'legitimate interests' as set out under the UK Data Protection Act.



3. SEARCH

3.1. ENSURING LAWFUL AND COMPLIANT SEARCH ACTIVITY

- Yes
- Partial
- No
- N/A

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Transactional Data (CUE / MID / MIAFTR)	●	●	●
Suspect Fraud Data*	●	●	●
Confirmed Fraud Data*	●	●	●

* Subject to successful due diligence completion.





3. SEARCH

3.2. SEARCH – ‘REASONABLE GROUNDS’

3.2.1. Ensuring Lawful and Compliant Search Activity



The below guidance applies to direct manual searches conducted by individuals against the Data held in the IFB System(s), where a pre-existing suspicion of fraud is required. For further guidance on bulk matching against bulk data outputs such as the Confirmed Fraud Data (inclusive of Automated Decision Making) and Generic Data Feed (GDF), please refer to Sections 4, 5 and 6 of this document.

3.2.2. Requirement

The IFB makes the industry Transactional, Suspect and Confirmed Fraud Data available to its Members to search against on a single-search basis, where a User has a pre-existing suspicion of fraud. Searches across the Data **must** only be used for the purposes of preventing, detecting and investigating fraud and complying with legal obligations.

3.2.3. Guiding Principle

The Data held by the IFB on the insurance industry's behalf includes Personal, Personal Sensitive and Special Category Data, which has added protections under GDPR. It is important that all Users treat this Data appropriately and sensitively. As such, searches conducted **must** be proportionate, legal, accountable and necessary, as well as premised on a 'reasonable grounds' to suspect fraud in line with 'legitimate interests' as set out under the UK Data Protection Act.

3.2.4. Authorised Users Must:

- 3.2.4.1. Only access the Data for the prevention and detection of crime as permitted under the Purpose and in line with the exemptions granted under the UK Data Protection Act. Searches must be valid, proportionate and targeted to the Data points in question.
- 3.2.4.2. Only conduct a search where a valid suspicion of fraud exists, based on a 'reasonable grounds' for suspicion.
- 3.2.4.3. Be able to articulate the reasonable grounds for suspicion in any given instance, based on known facts and information which are relevant to the likelihood that fraud has been committed and the person, Member organisation or article of interest is involved.
- 3.2.4.4. Only conduct a search where a claim, application or a provision of service has triggered a recognised industry fraud indicator or a case has been referred from the business in to the Member organisation's fraud team, and the fraud team has accepted the case for further investigation.
- 3.2.4.5. Ensure their search is sufficiently targeted to the Data Subject or target Data point in question, based on information already held by the Member. Be aware that their search activity is subject to compliance checks on a periodic and ad hoc basis.
- 3.2.4.6. Treat any intelligence Data, risk score or confirmed fraud match returned as indicative only, and further evidence any Data presented before a decision to void a policy or repudiate a claim is made.



3. SEARCH

3.2.5. Authorised Users Must Not:

- 3.2.5.1. Search for any other reason than outlined above. This includes searching for entities not linked to a fraud investigation, conducting speculative searches or phishing activity, or a User searching for themselves, friends or relatives, etc.
- 3.2.5.2. Conduct searches at First Notification of Loss (FNOL) or any other point in the policy or claims lifecycle (inclusive of application or renewal), where an existing suspicion of fraud is not already present.
- 3.2.5.3. Conduct searches for all claims over a certain value, where an existing suspicion of fraud is not already present.
- 3.2.5.4. Use the results of any search returned as a 'sole decision making factor', but as 'one tool among many' and an indication that further investigation is required in order to validate the match and ensure the appropriate decision is taken. Other enquiries **must** include searching other internal and external systems, databases and other relevant sources of information.
- 3.2.5.5. Undertake a search for any party that is not an existing Member of the IFB.

3.2.6. Interface Managers Must:

Assume responsibility within their Member organisation for:

- 3.2.6.1. Ensuring that robust and appropriate policies are in place to ensure searches are only conducted as outlined in Section 3 of the Membership Rules.
- 3.2.6.2. Ensuring all Data Subjects at the outset of their user journey have sight of the relevant Fair Processing Notices (FPNs), advising that their Data may be shared with fraud-prevention databases and agencies, where fraud is found.

3.2.7. Interface Managers Must Not:

Ignore, delay or postpone any communications or actions in respect of search requirements. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.

3.2.8. Governance

- 3.2.8.1. IFB will provide training on the use of the IFB Data and / or System(s) and the appropriate grounds to search.
- 3.2.8.2. An acknowledgment of each Authorised User and Interface Manager's responsibility to uphold the principle will be included in the annual attestation.
- 3.2.8.3. Compliance checks will be undertaken between IFB and Authorised Users. Authorised Users will be asked to talk through the reasons for a selection of searches, including identifying reasonable grounds and a legitimate interest, as detailed within the Rules.

Accountability – Authorised Users will be accountable for ensuring they are compliant with the principle. Compliance checks will place accountability on Users to explain the justification of their searches. Feedback can be provided to Interface Managers regarding potential learning needs that can support compliance.

Accessibility – Compliance checks may be undertaken remotely and directly with the relevant Authorised Users. Training and supporting documentation will be readily accessible online and presented in clear language to support Authorised Users in complying with the principle. New Authorised Users will be allocated the training as part of their onboarding as a prerequisite to gaining access.

Transparency – Compliance checks between Member and IFB support open conversation about the understanding of the Rules and how they should be applied. Those consistently failing to adhere to the principle subject to Measures as detailed in Section 16.



4.

Generic Data Feed

The Generic Data Feed (GDF) is a weekly Data output file that is provided to IFB customers consisting of suspect entity Data taken from distributed IFB products. Many customers derive the greatest value from IFB products by matching Data within internal databases and solutions, without the need for manual double keying.

Given the sensitivity of this Data, the highest standards of security and Data protection must be observed. Any matches to GDF intelligence Data must be treated as indicative only, subject to further validation on a Member's part.



4. GENERIC DATA FEED

4.1. GENERIC DATA FEED

4.1.1. Ensuring Integrity of the Bulk Intelligence Data

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Generic Data Feed*	●	●	●

* Subject to successful application and demonstration of technical capability to process the GDF file.





4. GENERIC DATA FEED

4.2. GENERIC DATA FEED

Ensuring Integrity of the Bulk Intelligence Data

4.2.1. Requirement

The Generic Data Feed (GDF) is a weekly Data output file that is provided to IFB customers consisting of suspect entity Data taken from distributed IFB products. Many customers derive the greatest value from IFB products by matching Data within internal databases and solutions, without the need for manual double keying. While the IFB maps all entities from issued intelligence products, the GDF cannot be used in isolation; customers are required to refer to the corresponding intelligence products and use the Data feed alongside these to fully understand the context and National Intelligence Model (NIM) grading.

4.2.2. Guiding Principle

Given the sensitivity of this Data, the highest standards of security and Data protection **must** be observed. Any matches to GDF intelligence Data **must** be treated as indicative only and are subject to further validation on a Member's part.

4.2.3. Authorised Users Must:

- 4.2.3.1. Only use the GDF in the form of an ingestion into a database and not as a direct look-up and / or reference source.
- 4.2.3.2. Only access the Data for the prevention and detection of crime as permitted under the Purpose and in line with the exemptions granted under the UK Data Protection Act.
- 4.2.3.3. Treat any match to intelligence Data as indicative only. Manual review is required to before a decision to void a policy or repudiate a claim is made.
- 4.2.3.4. Refer to the corresponding intelligence products relating to a match in order to fully understand the context and NIM grading.
- 4.2.3.5. Be aware that their activity in respect of the GDF is subject to compliance review on a periodic and ad hoc basis.

4.2.4. Authorised Users May:

Ingest the GDF in part rather than full, dependent on which tabs they find most helpful, as long as this is both:

- 4.2.4.1. Consistent week-on-week.
- 4.2.4.2. The hard delete tab is included each week (in the case of the new GDF format).

4.2.5. Authorised Users Must Not:

- 4.2.5.1. Use the results of any match to the download Data as a 'sole decision making factor', but an indicator that fraud might have previously been committed. Further investigation is required in order to validate the match and ensure the appropriate decision is taken.
- 4.2.5.2. Apply automated decision making to the Data, either in terms of declining or pricing business. All matches **must** be referred for human processing. Auto-alerting is however permitted.
- 4.2.5.3. Use or access the GDF on behalf of any party that is not an existing Member of the IFB.

4.2.6. Interface Managers Must:

Assume responsibility within their Member organisation for ensuring that:

- 4.2.6.1. The GDF is only used in the form of an ingestion into a database and not as a direct look-up and / or reference source.
- 4.2.6.2. The application form to start receiving the GDF is correctly completed.
- 4.2.6.3. Only designated role-holders are granted technical permissions to download the GDF file.
- 4.2.6.4. The GDF is only processed as outlined in Section 4 of this document.
- 4.2.6.5. The delta GDF Data files, issued weekly by the IFB, are ingested into their destination solution every seven days to ensure the Member is working from only the most up-to-date version of the file.
- 4.2.6.6. The GDF file is stored in a designated secure area and permanently deleted after ingest into internal counter-fraud solutions.
- 4.2.6.7. On IFB request, provide information about GDF processing, and change aspects of this processing if deemed non-compliant with enhanced requirements.

4.2.7. Interface Managers Must Not:

- 4.2.7.1. Ignore, delay or postpone any communications or actions in respect of GDF requirements. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.



4. GENERIC DATA FEED

4.2.8. Interface Managers Should:

- 4.2.8.1. In relation to the GDF, align their Data-retention limits to those of the IFB, as set out in the Section 17.2 of this document.

4.2.9. Governance

- 4.2.9.1. IFB will provide training on how to use the GDF in accordance with the Rules.
- 4.2.9.2. As part of the annual attestation, Authorised Users and Interface Managers will be required to confirm they understand how to appropriately use the GDF.
- 4.2.9.3. Interface Managers must demonstrate the existence of appropriate policies to help ensure data is accessed appropriately.

Accountability – Authorised Users must demonstrate an understanding of how the Data should be used. Interface Managers will provide evidence that there is internal oversight of how the GDF is used and take responsibility for the completion of compulsory training.

Accessibility – Training and supporting documentation will be readily accessible online for all roles. Training and attestation will be issued on an annual basis by the IFB. New Authorised Users will be allocated the training as part of their onboarding as a prerequisite to gaining access.

Transparency – Users and / or Members failing to adhere to the Rules subject to Measures as detailed in Section 16.



5.

Confirmed Fraud Data

The Confirmed Fraud Data can be downloaded as a separate file for use for screening policy and claims data (inclusive of Third Party Claims) throughout their respective lifecycles. This enables Members to integrate the Data with other fraud screening and data mining tools they might utilise internally.

Given the sensitivity on this Data, the highest standards of security and Data protection are required to ensure its appropriate use. Unless permitted within the scope of Automated Decision Making (as set out in Section 6 of this document), any matches to the Confirmed Fraud Data must be treated as indicative only and are subject to further manual validation on a Member's part.



5. CONFIRMED FRAUD DATA

5.1. CONFIRMED FRAUD DATA

5.1.1. Ensuring Appropriate Use of the Confirmed Fraud Data

	1 Full Member – Insurer	2 Full Member – Non Insurer [^]	3 Community Member
Confirmed Fraud Data download*	Yes (Green dot)	Partial (Yellow dot)	N/A (Grey dot)

* Subject to successful completion of due diligence.

[^] In the case of Non-Insurer Members, subject to successful application and demonstration of an applicable use case / technical capability to process the download file.



5. CONFIRMED FRAUD DATA

5.2. CONFIRMED FRAUD DATA

5.2.1. Ensuring Appropriate Use of the Confirmed Fraud Data



Fair and appropriate use of Confirmed Fraud Data is subject to the Rules in regard to both **standard processing** and **automated decision making**. The guidance in Section 5 applies to **standard processing** of the Confirmed Fraud Data, which is based on system alerting in combination with manual review and validation of any full or partial data matches identified at any point in the claim and policy lifecycle. This is distinct from **automated decision making**, whereby final outcomes may be reached using solely automated processes. Guidance to **automated decision making** is set out in Section 6 to this document. It is at the Member's discretion as to whether they opt to apply **standard processing** or **automated decision making** to the Confirmed Fraud Data, providing the Rules as set out in this document are adhered to in full.

5.2.2. Requirement

The Confirmed Fraud Data can be downloaded (by Authorised Users with technical permissions) as a separate file for use for screening against a Member's policy and claims data (inclusive of Third Party Claims) throughout their respective lifecycles. This enables Members to integrate the Data with other fraud screening and Data mining tools they might utilise internally.

5.2.3. Guiding Principle

Given the sensitivity on this Data, the highest standards of security and Data protection are required to ensure its appropriate use. Unless permitted within the scope of Automated Decision Making (per Section 6 of this document), any matches to the Confirmed Fraud Data must be treated as indicative only and are subject to further manual validation on a Member's part.

5.2.4. Authorised Users Must:

- 5.2.4.1. Only access the Data for the prevention and detection of crime as permitted under the Purpose and in line with the exemptions granted under the UK Data Protection Act.
- 5.2.4.2. Treat any Confirmed Fraud match returned as an indicator that fraud might have been previously committed. Further manual review is required to before a decision to void a policy or repudiate a claim is made.
- 5.2.4.3. Be aware that their activity in respect of the Confirmed Fraud Data is subject to compliance review on a periodic and ad hoc basis.
- 5.2.4.4. searching for themselves, friends or relatives, etc.

- 5.2.4.5. Conduct searches at First Notification of Loss (FNOL) or any other point in the policy or claims lifecycle (inclusive of application or renewal), where an existing suspicion of fraud is not already present.

5.2.5. Authorised Users Must Not:

- 5.2.5.1. Use the results of any match to the download Data as a 'sole decision making factor', but an indicator that fraud might have previously been committed. Further investigation is required in order to validate the match and ensure the appropriate decision is taken.
- 5.2.5.2. Use or access the download Data on behalf of any party that is not an existing Member of the IFB.
- 5.2.5.3. Use the Confirmed Fraud Data for marketing purposes.
- 5.2.5.4. In the case of Non-Insurer Members, use the Confirmed Fraud Data for the benefit of any non-IFB Members.



5. CONFIRMED FRAUD DATA

5.2.6. Interface Managers Must:

Assume responsibility within their Member organisation for ensuring that:

- 5.2.6.1. In the case of Non-Insurer Members, the application form to start receiving the Confirmed Fraud Data is correctly completed.
- 5.2.6.2. The download file is stored securely in a designated secure area and permanently deleted after ingest into internal counter-fraud solutions.
- 5.2.6.3. Robust and appropriate policies are in place to ensure the Confirmed Fraud Data is processed in line with Section 5 of this document.
- 5.2.6.4. Only those Authorised Users required are granted technical permissions to download the Confirmed Fraud Data file.
- 5.2.6.5. The Confirmed Fraud Data is only used in the form of an ingestion into a database and not as a direct look-up and / or reference source.
- 5.2.6.6. The Confirmed Fraud Data-retention period of seven days is fully observed so the Member is working from only the most up-to-date version.
- 5.2.6.7. In the case of Non-Insurer Members, use the Confirmed Fraud Data for the benefit of any non-IFB Members.
- 5.2.6.8. On IFB request, provide information about Confirmed Fraud Data processing and amend aspects of this processing, if deemed non-compliant with enhanced requirements

5.2.7. Interface Managers Must Not:

- 5.2.7.1. Ignore, delay or postpone any communications or actions in respect of download requirements. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.
- 5.2.7.2. Delegate any of the provisions set out in Section 5.6 to any other Authorised User.
- 5.2.7.3. Make any decision solely based on the provision of Section 5.6.

5.2.8. Interface Managers May:

- 5.2.8.1. Screen against the Confirmed Fraud Data file for the purpose of vetting potential new hires and bulk screening of members of staff.
- 5.2.8.2. Conduct a manual search against the Confirmed Fraud Data, where a Member is investigating a case of potential internal fraud and / or subjecting an employee to annual enhanced vetting.

5.2.9. Governance

- 5.2.9.1. Annual training and attestation for Authorised Users with access to the Confirmed Fraud Data is required of users, in order to demonstrate an understanding of their roles and responsibilities in using the Data.
- 5.2.9.2. Interface Managers must demonstrate the existence of appropriate policies to help ensure Data is accessed and used in accordance with the Rules.

Accountability – Authorised Users of the Data must demonstrate an understanding of how the Data should be used. Interface Managers will provide evidence that there is internal oversight of how Data is used and take responsibility for the completion of the compulsory training across their User base.

Accessibility – Training and supporting documentation will be readily accessible to all roles. Training and attestation will be issued on an annual basis by IFB. New Authorised Users will be allocated the training as part of their onboarding as a prerequisite to gaining access. Appropriate policies can be provided digitally to the IFB as part of onboarding. Appropriate policies can be provided digitally to the IFB as part of onboarding or an ad hoc request thereafter.

Transparency – Users and Members failing to adhere to the principle may be subject to Measures as detailed in Section 16.



6.

Automated Decision Making

Members are permitted to use the Confirmed Fraud Data for the purposes of automated decision making (a) at the point of providing a quote to a customer; (b) during the pre-sale stage; and/or (c) at the point-of-sale stage, providing that the Rules and all relevant Data protection legislation are observed in full.

Members may apply automated decision making to Confirmed Fraud Data, provided that all specified controls, ethical safeguards, and Data protection laws are met, ensuring transparency, subject notification, and the opportunity for manual review where appropriate.



6. AUTOMATED DECISION MAKING

6.1. AUTOMATED DECISION MAKING

6.1.1. Use of Automated Decision Making Against Confirmed Fraud Data

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Automated Decision Making*	● Yes	● Partial	● N/A

* In the case of Non-Insurer Members, subject to successful application and demonstration of use case / technical capability to process the Confirmed Fraud download file.



6. AUTOMATED DECISION MAKING

6.2. AUTOMATED DECISION MAKING

6.2.1. Use of Automated Decision Making Against Confirmed Fraud Data



In the context of the Membership Rules, automated decision making specifically refers to systems and processes that a) make the **final decision** about a **fraud outcome** (for example, as used in respect of new or existing policies, including any changes to the policy status or pricing) and b) directly impact a Data subject without prior human / manual review or intervention.

Automated decision making does not include use of systems that assist in the **process leading up** to the final decision, such as sending alerts, sorting or triaging claims, or removing items from straight-through workflows that process claims up to the point of final outcome.

These process-supporting actions are permitted and are not restricted by the rules on automated decision making.

The rules in this Section only apply to systems and processes that make the **final, binding decisions** – i.e. the ones that directly and significantly impact a Data Subject, such as determining their policy status, or the pricing of their policy at (a) at the point of providing a quote to a customer; (b) during the pre-sale stage; and/or (c) at the point-of-sale stage. Automated decision making is **not permitted** at Post-Sale stage, or in respect of Claims Data or Mid-Term Adjustments. In such instances, the guidance on **standard processing** around the Confirmed Fraud Data applies, which is set out in Section 5 of this document.

6.2.2. Requirement

Members are permitted to use the Confirmed Fraud Data for the purposes of automated decision making (a) at the point of providing a quote to a customer; (b) during the pre-sale stage; and/or (c) at the point-of-sale stage, providing that the below Rules and all relevant Data protection legislation are observed in full.

6.2.3. Principle

Members may apply automated decision making to Confirmed Fraud Data, provided that all specified controls, ethical safeguards and Data protection laws are met, ensuring transparency, subject notification, and the opportunity for manual review where appropriate.

6.2.4. Heads of Fraud and Interface Managers Must:

- 6.2.4.1. Inform the IFB if they intend to automate any matching investigation process involving the Confirmed Fraud Data.
- 6.2.4.2. Ensure there is a documented legal basis set out internally for any automated decision making processes, in line with the Purpose as set out in section 1.4 of this document.
- 6.2.4.3. Ensure that automated decision making is applied only (a) at the point of providing a quote to a customer; (b) during the pre-sale stage; and/or (c) at the point-of-sale stage.

6.2.4.4. Ensure that any matching conducted is multifactorial in nature, as opposed to based on single Data point matches. In the case of single Data point matches (inclusive of Articles of Fraud), these should be referred for manual review. In such instances, the Rules around standard processing of the Confirmed Fraud Data, as set out in Section 5, apply.

6.2.4.5. Be able to evidence the factors being used in any governance review and on Data Subject or IFB request.

6.2.4.6. Ensure that automated decision making logic should be of sufficient sophistication to effectively replicate a human decision.

6.2.4.7. Ensure that all processing involving the Confirmed Fraud Data is ethical and safeguards the rights of Data Subjects.

6.2.4.8. Establish robust controls to monitor the performance of outcomes when Confirmed Fraud Data is used in automated processes, including ongoing monitoring with structured governance and tracking deviations between automated and manual decision results.



6. AUTOMATED DECISION MAKING

- 6.2.4.9. Include in Fair Processing Notices (FPNs) that automated decision making may occur as part of processing Personal Data, particular in respect of the identifying fraud. Data Subjects must be informed of their rights to request manual review in respect of automated decisions reached and provided with contact details for more information.
- 6.2.4.10. Maintain appropriate audit trails and Management Information (MI) capturing the outcomes automated decisions made using the Confirmed Fraud Data.
- 6.2.4.11. Periodically subject the logs of automated decisions to review, to ensure that the logic in place is working correctly and consistently.
- 6.2.4.12. Ensure any automated decision making conducted adheres to all relevant laws and the Membership Rules.
- 6.2.5.3. Apply automated decision making to anything other than the Confirmed Fraud Data only.
- 6.2.5.4. Allow solely automated decision making processes to in any way compromise adherence to the Membership Agreement.
- 6.2.5.5. Use automated decision making in any other context than as outlined above, for example direct marketing.
- 6.2.5.6. Use automated decision at Post-Sale stage, where referral for manual review is still required.
- 6.2.5.7. Apply automated decision making in respect of Mid-Term Adjustments or claim repudiation. In such instances, the Rules around standard processing of the Confirmed Fraud Data, as set out in Section 5, apply.
- 6.2.5.8. Load re-filings on the basis of match to the Confirmed Fraud System on an automated basis. Any prospective re-loadings identified as a result of an automated decision must still undergo manual review before re-filing.

6.2.5. Heads of Fraud and Interface Managers

Must Not:

- 6.2.5.1. Automate any processes in respect of review and approval of Suspect Fraud, where the requirement for manual review applies.
- 6.2.5.2. Automate any decision making processes without first notifying the IFB and ensuring the process is ethical, compliant with the terms of the Membership Rules and Membership Agreement and with all applicable Data protection laws and regulations.
- 6.2.5.9. Act in breach, or allow Authorised Users to act in breach, of any of the requirements set out Section 6 of these Rules.
- 6.2.5.10. Ignore, delay or postpone any communications, reporting or actions in respect of automated decision making requirements. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.



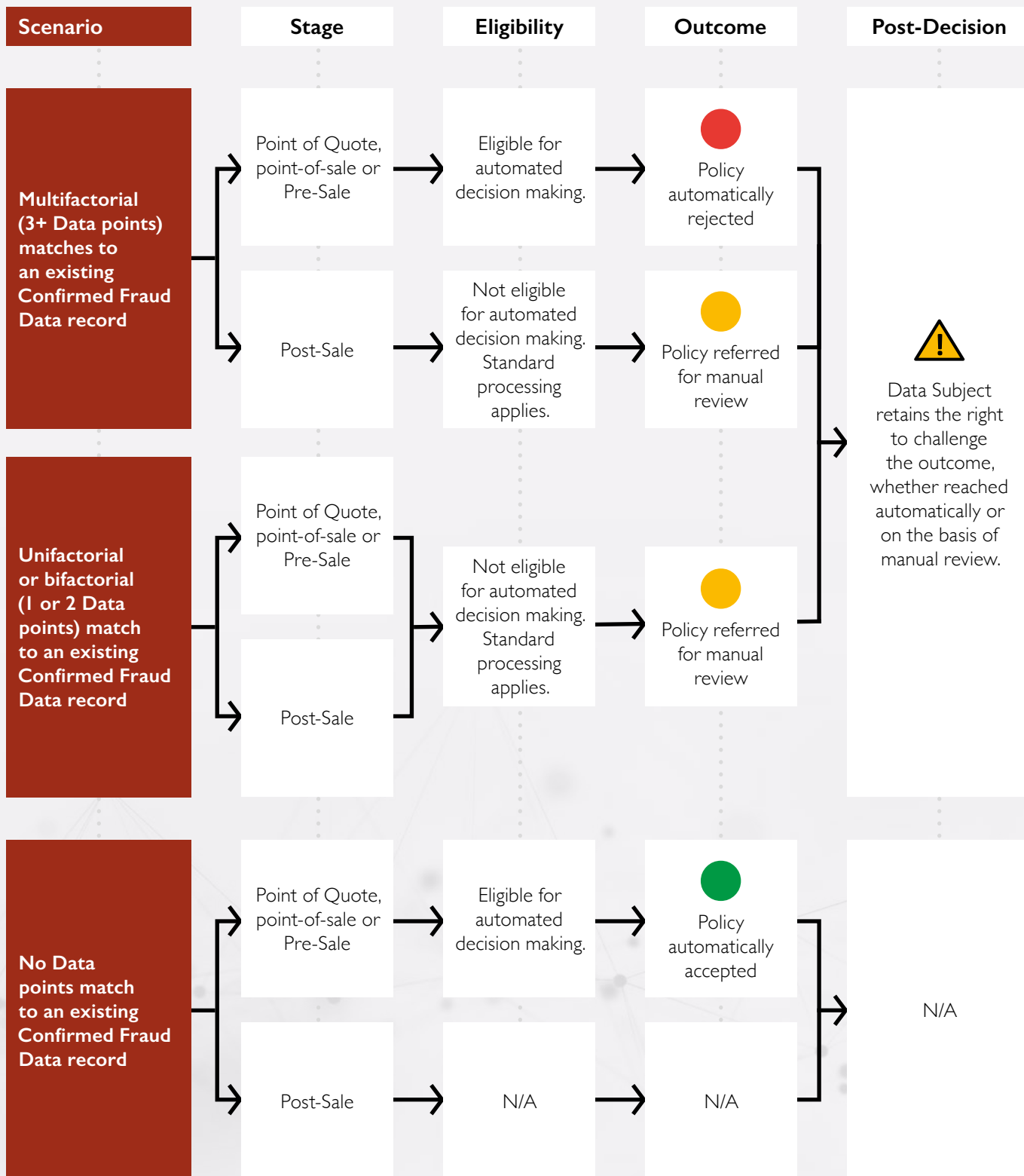
The IFB reserves the right, based on immediate and / or significant risk identified to other members, to revoke a Member's right to conduct automated decision making, in the event of any breaches of the Rules, as set out in this Section 6.



6. AUTOMATED DECISION MAKING

6.3. AUTOMATED DECISION MAKING

6.3.1. Use of Automated Decision Making Against Confirmed Fraud Data





6. AUTOMATED DECISION MAKING

6.3.2. Governance

- 6.3.2.1. The Head of Fraud or Interface Manager must notify the IFB if a Member intends to implement automated decision making. This should be accompanied by confirmation that the decision making process will meet the criteria set out in the Rules.
- 6.3.2.2. As part of the annual attestation, the Head of Fraud and Interface Manager must confirm that any decision making process being applied meets the criteria set out in the Rules.

Accountability – The Head of Fraud and Interface Manager will be responsible for ensuring adherence with the Rules around automated decision making. Members are free to implement automated decision making at their discretion, but do so in the acknowledgement it must be done in adherence with the Rules.

Accessibility – The Rules and annual attestation will set out the expectations of how automated decision making can be used and the responsibilities of the Head of Fraud and Interface Manager. The annual attestation will be applicable for all Heads of Fraud and Interface Managers, regardless of whether automated decision making is being implemented. This will ensure Heads of Fraud and Interface Managers are aware of their responsibilities should they wish to plan to implement it in the future.

Transparency – Requiring Heads of Fraud and Interface Managers from all Members to acknowledge an understanding of the Rules relating to Automated Decision Making, regardless of whether it is currently being applied, helps develop a consistent understanding across the Membership and build confidence that Members are applying Automated Decision Making in a consistent manner.



7.

Data Disclosure

The IFB and its Members are able to share information purely for the purpose of detecting and preventing fraud. All role holders – both IFB staff and Members – must adhere to the National Intelligence Model (NIM) in terms of intelligence grading, handling codes and IFB requirements around onward sharing of Data, where permitted. The consequences of a Data Breach could pose a significant threat to the IFB and its Membership, so it is imperative that Users adhere to the same set of standards at all times, only disclosing Data on an onward basis where explicitly permitted to do so.

The IFB data-sharing model is only as strong as the weakest link in the chain; all Roles have a responsibility for safeguarding the Data and ensuring that onward sharing only takes place when explicitly authorised by the IFB via the NIM grading assigned.



7. DATA DISCLOSURE

7.1. DATA DISCLOSURE

7.1.1. Ensuring Compliant Onward Data Disclosure

- Yes
- Partial
- No
- N/A

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Transactional Data (CUE / MID / MIAFTR)	●	●	●
Suspect Fraud Data*	●	●	●
Confirmed Fraud Data*	●	●	●

* Subject to successful due diligence completion.



7. DATA DISCLOSURE

7.2. DATA DISCLOSURE

Ensuring Compliant Onward Data Disclosure

7.2.1. Requirement

The IFB and its Members are able to share information purely for the purpose of detecting and preventing fraud. All role holders – both IFB staff and Members – **must** adhere to the National Intelligence Model ('NIM') in terms of intelligence grading, handling codes and IFB requirements around onward sharing of Data, where permitted. The consequences of a Data Breach could pose a significant threat to the IFB and its Membership, so it is imperative that Users adhere to the same set of standards at all times, only disclosing Data on an onward basis where explicitly permitted to do so.

7.2.2. Guiding Principle

The IFB data-sharing model is only as strong as the weakest link in the chain; all Authorised Users have a responsibility for safeguarding the Data and ensuring that onward sharing only takes place when explicitly authorised by the IFB via the NIM classification assigned.

7.2.3. Authorised Users Must:

- 7.2.3.1. Adhere in full to the NIM in terms of intelligence handling, which forms part of the onboarding and IFB e-learning training package.
- 7.2.3.2. Undertake additional research to corroborate intelligence, using the intelligence to inform fraud investigation strategies and to identify claims and policies with potential fraud concerns.
- 7.2.3.3. If in doubt, query with the IFB whether they can disclose Data or not in any given scenario.
- 7.2.3.4. Immediately report any instances of actual, suspected or threatened unauthorised disclosure, misappropriation, misuse, loss, corruption, damage to, deletion of, or Data Breach in respect of any of the Data to their designated Interface Manager and Head of Fraud.

7.2.4. Authorised Users May:

- 7.2.4.1. Share Data accessed via IFB across counter-fraud teams within their Member organisation and with representatives or delegated authorities working on their behalf, e.g. claim handlers, where the NIM rating specifically allowed for sharing of the Data outside of internal Member fraud teams or dedicated counter-fraud personnel. In such instances, Data shared with representatives **must** only contain information relevant to the investigation in question and must be destroyed once the investigation has been completed.
- 7.2.4.2. Reference Data sourced from the IFB – either via an online search look-up or via an IFB-issued product – within a fraud report. However, information **must** only be in the context of a wider investigation process based on a number of investigative tools. Any Data accessed, in particular in respect of IFB System(s), would need to be further evidenced before a decision is made.

7.2.5. Authorised Users Must Not:

- 7.2.5.1. Publish, disclose or divulge any Personal Data to any third party, other than listed above. This includes the Data Subject to whom the Data relates.
- 7.2.5.2. Share Data outside of the above parameters and beyond the NIM handling instructions.
- 7.2.5.3. Share Data with representatives working on their behalf that is not relevant to the investigation in question. For this reason, it is strictly prohibited to provide such representatives with any and all bulk Data outputs.
- 7.2.5.4. Disclose IFB Transactional Data as the source of information. The IFB analytics solution contains aggregated Data from core industry databases such as MID, CUE and MIAFTR; these are the sources of any information obtained, and as such **must** be referenced as the source.
- 7.2.5.5. Attempt to contact a policyholder or claimant to raise concerns in respect of the intelligence.
- 7.2.5.6. Disclose the intelligence as part of any court proceedings.
- 7.2.5.7. Attempt to identify and contact the source of the intelligence.



7. DATA DISCLOSURE

7.2.6. Interface Managers May:

Share the Data with third party technology providers, provided that:

- 7.2.6.1. The Member has entered into a supplier agreement that is equivalent to the terms of the Membership Agreement.
- 7.2.6.2. The Data is subject to the same information security and Data protection standards as set out in the Membership Rules and Membership Agreement.
- 7.2.6.3. The Member acknowledges that they would retain liability in the event of any third-party Data Breach.
- 7.2.6.4. Where Data is subject to NIM grading, the relevant handling instruction are complied with.

7.2.7. Interface Managers Must:

- 7.2.7.1. Report any instances of actual, suspected or threatened unauthorised disclosure, misappropriation, misuse, loss, corruption, damage to, deletion of, or Data Breach in respect of any of the Data to the IFB within 24 hours.
- 7.2.7.2. Assume responsibility for ensuring that no access to the Data in bulk outputs are provided to any other teams or individuals who sit outside of the fraud or intelligence functions.

7.2.8. Interface Managers Must Not

- 7.2.8.1. Ignore, delay or postpone any communications, reporting or actions in respect of Data disclosure requirements. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.

7.2.9. Governance

- 7.2.9.1. All Authorised Users must undertake annual training on NIM to support the security of industry Data.
- 7.2.9.2. To encourage the safeguarding of industry data across Members, the training may also be offered to staff outside Member fraud teams.
- 7.2.9.3. Interface Managers must demonstrate the existence of appropriate policies to help ensure compliance with the principle.

Accountability – Authorised Users of the Data must demonstrate an understanding of how industry Data should be handled and shared. Interface Managers must take responsibility for ensuring training is completed by all Authorised Users and that appropriate internal processes exist.

Accessibility – Training and supporting documentation will be readily accessible online for all Users. Training and attestation will be issued on an annual basis by the IFB. New Users will be allocated the training as part of their onboarding as a prerequisite to gaining access to IFB Data.

Transparency – As a prerequisite of obtaining access to IFB Data and / or System(s), Members must demonstrate the existence of appropriate procedures and all Authorised Users must undertake IFB training. This approach will ensure all Members are confident that the same level of compliance exists across the industry. Measures for Data Breaches are outlined in Section 16.



8.

Ensuring Reciprocity

As a condition of Membership, all Members are required to contribute, collaborate, and reciprocate with the IFB using 'all reasonable endeavours'. It is recognised that reciprocity takes a number of forms, from broader intelligence sharing, to direct contribution to the Confirmed and Suspect reciprocal System(s), to the pooling of Data via ad hoc Data models. In addition, reciprocal activity may take the form of strategic engagement activities led by the IFB, such as participation in a Member Working Group, support of a PR campaign or contribution to the Strategic Threat Assessment.

In joining the IFB, the Member commits to adopting an 'all reasonable endeavours' approach to contributing to the IFB in as many forms as reasonably possible, in a fair, proportionate and consistent manner. Persistent 'zero' or 'token' contributors will be deemed as failing to meet the expected requirements of Membership to the Bureau.



8. ENSURING RECIPROCITY

8.1. ENSURING RECIPROCITY

8.1.1. Ensuring Fair and Proportional Contribution

- Yes
- Partial
- No
- N/A

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Intelligence sharing (IISs, misc intel)	●	●	●
Feedback submissions	●	●	●
Contribution to Suspect Fraud System*	●	●	●
Contribution to Confirmed Fraud System*	●	●	●
Contribution to ad hoc Data models [^]	●	●	●
Strategic engagement [^]	●	●	●

* Subject to successful completion of due diligence.

** For example, the Application Fraud Model, the Commercial Fraud Model, Data Vishing, Op Fenwood, or other ad hoc data sharing models.

[^] Such as participation in a Member Working Group, support of a PR campaign, or contributing to the Strategic Threat Assessment.



8. ENSURING RECIPROCITY

8.2. ENSURING RECIPROCITY

Ensuring Fair and Proportional Contribution

8.2.1. Requirement

As a condition of Membership, all Members are required to contribute, collaborate and reciprocate with the IFB using 'all reasonable endeavours'. It is recognised that reciprocity takes a number of forms, from broader intelligence sharing, to direct contribution to the Confirmed and Suspect reciprocal System(s), to the pooling of Data via ad hoc Data models. In addition, reciprocal activity may take the form of strategic engagement activities led by the IFB, such as participation in a Member Working Group, support of a PR campaign, or contribution to the Strategic Threat Assessment.

In joining the IFB, the Member commits to adopting an 'all reasonable endeavours' approach to contributing to the IFB in as many forms as reasonably possible, in a fair, proportionate and consistent manner. Persistent 'zero' or 'token' contributors will be deemed as failing to meet the expected requirements of Membership to the Bureau.

8.2.2. Guiding Principle

Reciprocity – in all its guises – constitutes a cornerstone of the IFB. The more Members pool their intelligence, knowledge and best practice, the stronger the industry stands against fraud. Fostering trust, mutual support, and active collaboration among Members is crucial to the sustained success of both the IFB data-sharing model and the industry's overarching counter-fraud strategy.

8.2.3. Heads of Fraud Must:

8.2.3.1. Assume full accountability within the organisation for ensuring that an 'all reasonable endeavours' approach to IFB contribution is consistently maintained.

8.2.3.2. Support the Interface Manager in the execution of this role, serving as escalation point for any concerns raised by the Interface Manager or the IFB.

8.2.4. Heads of Fraud Should:

8.2.4.1. Support the Interface Manager in progressing the internal adoption of bulk loading capabilities, in order to automate and drive efficiencies in the process.

8.2.5. Interface Managers Must:

8.2.5.1. Assume responsibility within the Member organisation for ensuring that robust appropriate policies are in place internally to govern fair and proportionate contribution to the IFB across all key areas. Actively participate in Customer Relationship Management (CRM) meetings, to include a review and understanding of relevant Management Information (MI) detailing Member contribution across all key areas. The Interface Manager is responsible for ensuring that any gaps in reciprocity are communicated internally within the Member organisation, and a plan of action to increase contribution put into place.

8.2.6. Interface Managers Should:

Assume responsibility within the Member organisation for ensuring that:

8.2.6.1. A fair and proportionate volume of eligible Confirmed and Suspect Fraud cases are loaded to the reciprocal System(s), in volumes commensurate to its size, market share, and risk appetite, according to its Membership type.

8.2.6.2. Initial loading activity is commenced and incrementally increased within a timescale agreed between the IFB and the Member, from the point of joining the respective System(s).

8.2.6.3. Eligible cases of Suspect and Confirmed Fraud are loaded regularly and consistently over time, without undue delay between fraud identification and fraud loading.

8.2.6.4. A reasonable and proportionate split of eligible cases of Suspect and Confirmed Fraud contributed across both claims and policy fraud.

8.2.6.5. Eligible cases of Suspect and Confirmed Fraud are loaded across all primary product lines underwritten within their Member organisation.

8.2.6.6. Feedback and IFB Intelligence Submissions (IISs) are submitted to the IFB in a regular and timely manner.

8.2.6.7. Contributions are made regularly and consistently to the IFB's suite of ad hoc Data models, as required.

8.2.6.8. The Member actively engages with the IFB on a more strategic level, for example by ensuring attendance of IFB Intelligence Forums, participation in Member Working Groups, contribution to the IFB's Strategic Threat Assessment, support of a PR campaign, and / or other forms of engagement requested by the IFB from time to time.



8. ENSURING RECIPROCITY

8.2.7. Interface Managers Must Not:

- 8.2.7.1. Ignore, delay or postpone any communications or actions in respect of contribution and reciprocity. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.

8.2.8. Interface Managers May:

- 8.2.8.1. Exercise discretion in respect of individual cases, opting not to load a case in certain instances in line with internal risk appetite.

8.2.9. Authorised Users Should:

- 8.2.9.1. Contribute a proportion of their Confirmed and Suspect Fraud cases, which meet the respective Fraud Definitions (as set out in Section 17.1 of this document), to the reciprocal System(s).
- 8.2.9.2. Co-operate with reasonable requests from the IFB and IFB Members to provide further details regarding a record loaded to the System(s).
- 8.2.9.3. Load as many cases as possible of Confirmed and Suspect Fraud cases, which meet the respective Fraud Definitions, to the reciprocal System(s), in line with Member risk appetite.
- 8.2.9.4. Respond to IFB-issued Feedback Requests in a timely manner.
- 8.2.9.5. Regularly submit IISs to the IFB for further investigation.
- 8.2.9.6. Provide a timely response to requests for ad hoc feedback (e.g. in respect of different Data models) where requested by IFB from time to time.
- 8.2.9.7. Seek to engage directly with the IFB where the Member has suspicions or indications of new or emergent patterns and modus operandi.
- 8.2.9.8. Minimise the need to make calls to other Members by adding as much information as they have available when loading a record.
- 8.2.9.9. Attend IFB events and forums, take part in wider strategic engagement with the IFB, where nominated to do so by the Interface Manager.

8.2.10. Authorised Users Should Not:

- 8.2.10.1. Leave Feedback Requests unanswered, where they hold intelligence relevant to the report in question.
- 8.2.10.2. Deliberately withhold loadings of Confirmed and Suspect Fraud cases, which meet the respective Fraud Definitions, from the reciprocal System(s).
- 8.2.10.3. Unduly delay loadings of Confirmed and Suspect Fraud cases, which meet the respective Fraud Definitions, to the reciprocal System(s).
- 8.2.10.4. Load multiple instances of the same article of fraud to the reciprocal System(s).
- 8.2.10.5. Fail to submit an IIS to the IFB, where there is a potential that the IFB could add value in respect of an investigation into organised cross-industry fraud.

8.2.11. Governance

- 8.2.11.1. Quarterly reviews of contributions will be discussed as part of Customer Relation Management (CRM) meetings.
- 8.2.11.2. IFB will support Members in their efforts to increase their contributions to the Suspect and Confirmed Fraud System(s), as well as increase engagement with / submissions to IFB in general.
- 8.2.11.3. Members will be encouraged to share their volumes of Suspect and Confirmed Fraud cases to encourage contributions from all Members.
- 8.2.11.4. The creation of a Reciprocity Working Group to promote and oversee improvements to reciprocity.

Accountability – IFB and Interface Managers will take accountability for encouraging reciprocity.

Accessibility – Members will be provided with analysis of their contributions and provided with support from the IFB to increase contributions.

Transparency – The review of contributions will take a broad view, incorporating loadings to the Suspect and Confirmed Data, in addition to other contributions, such as feedback, events and media campaigns, etc. This will support a holistic view of where individual Members are contributing. Any Member supporting the Reciprocity Working Group must commit to publishing their level of engagement with the IFB.



9.

Loading – Thresholds

The success of the reciprocal data-sharing model relies on the integrity of the Data within the System(s) and, as such, all Members need to work to the controls as set out within the Membership Rules and the Membership Agreement.

The Confirmed and Suspect Fraud Definitions need to be closely adhered to by all role holders at all times, with processes in place to ensure two-tier review ahead of loading a case to the reciprocal System(s).



9. LOADING – THRESHOLDS

9.1. LOADING – THRESHOLDS

9.1.1. Ensuring the Integrity of Data Loaded

- Yes
- Partial
- No
- N/A

1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
-------------------------	-----------------------------	--------------------

Transactional Data (CUE / MID / MIAFTR)	●	●	●
Suspect Fraud Data*	●	●	●
Confirmed Fraud Data*	●	●	●





9.2. LOADING – THRESHOLDS

Ensuring the Integrity of Data Loaded

9.2.1. Requirement

The success of the reciprocal data-sharing model relies on the integrity of the Data within the System(s) and, as such, all Members need to work to the controls as set out within the Membership Rules and the Membership Agreement.

9.2.2. Guiding Principle

The Confirmed and Suspect Fraud Definitions, as set out in Section 17.1 of this document, need to be closely adhered to by all role holders at all times, with processes in place to ensure two-tier review ahead of loading a case to the reciprocal System(s).

9.2.3. Authorised Users Must:

In instances of Confirmed Fraud:

- 9.2.3.1. Ensure two-person review takes place ahead of loading any case to the Confirmed Fraud System. The second level review and sign-off must be conducted by an appropriately senior resource on a Member's fraud team.
- 9.2.3.2. Ensure that fraud has been evidenced to a 'balance of probabilities' basis (as opposed to 'beyond all reasonable doubt') and that one of eight applicable fraud outcomes, as set out in the Confirmed Fraud Definition, has been reached. This outcomes include: active repudiation, a policy voidance, or a cancellation relying on the fraud condition. Police action or court litigation are not pre-requisites to load to the System.
- 9.2.3.3. Ensure that an appropriately worded correspondence is issued to the Data Subject emphasising the fraud outcome.
- 9.2.3.4. Ensure that victim Data is not loaded to the System. In instances of identity theft, only the Data pertaining to the fraudster can be loaded as articles of fraud, e.g. the email address or bank account.

9.2.4. Authorised Users Must:

In instances of Suspect Fraud:

- 9.2.4.1. Ensure two-tier review takes place ahead of loading any case to the Suspect Fraud reciprocal Data set. The first level of review can be manual review or system-driven, provided that a second-tier manual review takes place to validate the suspicion before a loading is made. This manual review **must** be conducted by an appropriately trained resource on a Member's fraud team.
- 9.2.4.2. Ensure that there are reasonable grounds for the suspicion, based on known facts and information which are relevant to the likelihood that fraud has been committed and the person, business or article of interest is involved.
- 9.2.4.3. Ensure that the correct NIM grading is applied.
- 9.2.4.4. Ensure no victim Data is loaded without prior written consent of the Data Subject.

9.2.5. Authorised Users May:

- 9.2.5.1. Load third party claimants to the reciprocal System(s), providing they have had sight of relevant Fair Processing Notices (FPNs) as part of their prior User journey, advising that their Data may be shared with fraud-prevention databases and agencies, where fraud is found.

9.2.6. Authorised Users Must Not:

- 9.2.6.1. Load cases of either Suspect or Confirmed Fraud retrospectively. A case can only be loaded if the Fraud Definition date falls after the Member join date.
- 9.2.6.2. Load details of a Data Subject who is under 17 years of age.
- 9.2.6.3. Load victim Data to the respective Systems, except as outlined in Section 9.3 above.
- 9.2.6.4. Load cases of fraud to the Confirmed Fraud System, where the Data Subject in question is a 'walkaway'. However, Members **may** rely on the policyholder's failure to respond to the letter outlining the results of the investigation as evidence in support of a filing.



9. LOADING – THRESHOLDS

9.2.7. Interface Managers Must:

- 9.2.7.1. Assume responsibility within their Member organisation for ensuring processes are in place to ensure only cases that meet the respective Fraud Definitions are loaded to the reciprocal System(s).
- 9.2.7.2. Ensure that the first 15 Confirmed or Suspect Fraud cases identified for loading are reviewed by the IFB and approved for loading to the System(s).
- 9.2.7.3. Co-operate with reasonable requests from the IFB and IFB Members to provide further details regarding a record loaded to the System(s).

9.2.8. Interface Managers Must Not:

- 9.2.8.1. Ignore, delay or postpone any communications or actions in respect of loading threshold requirements. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.

9.2.9. Governance

- 9.2.9.1. Guidance on the Confirmed and Suspect Fraud Definitions will be made clear in annual compulsory training.
- 9.2.9.2. An acknowledgment of each Authorised User's responsibility to upholding the principle will be included in the annual attestation.
- 9.2.9.3. Interface Managers will be responsible for providing the IFB evidence of a formal process in place to support two-person review. This must be demonstrated annually to retain access.
- 9.2.9.4. Compliance checks will take place on a quarterly basis where members must demonstrate the threshold for loading has been met on a selection of cases.

Accountability – All Authorised Users will be clear about their responsibilities to adhere to the respective Fraud Definitions. The IFB will support Members through annual training, so that all Authorised Users are trained to the same required standard. Members may be subject to Measures if data is loaded incorrectly, as detailed in Section 16.

Accessibility – Training and supporting documentation will be readily accessible online for all Authorised Users. Training and attestation will be issued on an annual basis by IFB. New Authorised Users will be allocated the training as part of their onboarding. Appropriate policies can be provided digitally to the IFB as part of onboarding, or as part of scheduled audit activity and / or on ad hoc request thereafter.

Transparency – As a prerequisite of obtaining access to the Confirmed and Suspect Fraud Data, Members must demonstrate the existence of appropriate procedures, and all Authorised Users must have undertaken IFB training. This approach will ensure all Members are confident that the same level of oversight exists across the industry.



10.

Loading – Transparency

Transparency in respect of the Confirmed Fraud Data is of paramount importance, and assists in promoting the deterrent message, which is one of the main objectives of the register. Each Member's Fair Processing Notices (FPNs) must advise customers that their details may be shared with other agencies and databases for the purpose of detecting and preventing fraud. Where a claimant is represented, responsibility lies with their solicitor for communicating FPN information to their client.

In the instance of Suspect Fraud loadings, Data Subjects will not be explicitly informed that their details have been loaded to the System. However, Members will be required to demonstrate compliant FPNs are in place informing customers how their Personal Data is obtained and used, including the sharing of Data with fraud-prevention databases and agencies where appropriate.



10. LOADING – TRANSPARENCY

10.1. LOADING – TRANSPARENCY

10.1.1. Ensuring Appropriate Transparency Towards Data Subjects

- Yes
- Partial
- No
- N/A

1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
----------------------------	-----------------------------------	-----------------------

Transactional Data (CUE / MID / MIAFTR)	●	●	●
Suspect Fraud Data*	●	●	●
Confirmed Fraud Data*	●	●	●





10. LOADING – TRANSPARENCY

10.2. LOADING – TRANSPARENCY

Ensuring Appropriate Transparency Towards Data Subjects

10.2.1. Requirement

Transparency in respect of the Confirmed Fraud Data is of paramount importance, and assists in promoting the deterrent message, which is one of the main objectives of the register. Each Member's Fair Processing Notices (FPNs) **must** advise customers that their details may be shared with other agencies and databases for the purpose of detecting and preventing fraud. Where a claimant is represented, responsibility lies with their solicitor for communicating FPN information to their client.

In the instance of Suspect Fraud loadings, Data Subjects will not be explicitly informed that their details have been loaded to the System, given the System is envisaged to be a covert one, the existence of which will not be made overtly public. However, Members will be required to demonstrate compliant FPNs in place informing customers how their Personal Data is obtained and used, including the sharing of Data with fraud-prevention databases and agencies where appropriate.

10.2.2. Guiding Principle

Data Subjects **must** be appropriately informed via a combination of FPN content and – in the case of Confirmed Fraud loadings – proactive outbound communication.

10.2.3. Authorised Users Must:

- 10.2.3.1. Provide clear and transparent communication to the Data Subject in the case of Confirmed Fraud loadings, advising of the breach of the fraud condition and the specific fraud outcome reached.

10.2.4. Authorised Users Should:

- 10.2.4.1. In addition to confirming the fraud outcome, reference in their communication to the Data Subject that their details are being loaded to the Confirmed Fraud System. However, for the avoidance of doubt, this does not represent an obligation at this time.

10.2.5. Authorised Users Must Not:

- 10.2.5.1. Issue communication to the Data Subject in the case of Confirmed Fraud loadings that is insufficiently clear or does not appropriately emphasise the breach of the fraud condition and the specific fraud outcome reached.

10.2.6. Heads of Fraud Must:

- 10.2.6.1. Assume responsibility for ensuring their Member organisation's FPNs appropriately advise customers that their details may be shared with other agencies and databases for the purpose of detecting and preventing fraud.

10.2.7. Interface Managers Must Not:

- 10.2.7.1. Ignore, delay or postpone any communications or actions in respect of loading transparency requirements. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.

10.2.8. Governance

- 10.2.8.1. Interface Managers must demonstrate the existence of appropriate FPNs prior to obtaining access to the IFB Data and / or System(s) This must be demonstrated annually to retain access.

Accountability – Interface Managers will take responsibility that FPNs are in place and will form part of their roles and responsibilities.

Accessibility – Appropriate policies can be provided digitally to the IFB as part of onboarding, appropriate policies can be provided digitally to the IFB as part of onboarding or an ad hoc request thereafter.

Transparency – The existence of FPNs will be a prerequisite to obtaining access to the IFB Data and / or System(s) and must be demonstrated annually. This will help develop confidence across Members as to the integrity of loadings.



11.

Loading – Accuracy

Data must be accurate, up-to-date, adequate, relevant, objective, factual, clear, concise, not excessive and not kept for longer than is necessary for the Purpose. Processing must be fair and lawful, and shall comply with all relevant Data protection legislations. Members must delete and / or amend any records identified as having been incorrectly loaded by their Member organisation, and ensure records are kept up-to-date as required. Data accuracy is of utmost importance and must form part of the loading review stage and User compliance review processes.

The success of the fraud data-sharing model relies on the integrity of the Data submitted, and it is imperative that Members maintain, update and delete records as appropriate to ensure that the highest standards of Data accuracy are adhered to.



II. LOADING – ACCURACY

II.I. LOADING – ACCURACY

II.I.I. Maintaining the Accuracy and Relevancy of Data Loaded

- Yes
- Partial
- No
- N/A

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Transactional Data (CUE / MID / MIAFTR)	●	●	●
Suspect Fraud Data*	●	●	●
Confirmed Fraud Data*	●	●	●

* Subject to successful due diligence completion.



II. LOADING – ACCURACY

II.2. LOADING – ACCURACY

Maintaining the Accuracy and Relevancy of Data Loaded

II.2.1. Requirement

Data **must** be accurate, up-to-date, adequate, relevant, objective, factual, clear, concise, not excessive and not kept for longer than is necessary for the Purpose. Processing **must** be fair and lawful, and shall comply with all relevant Data protection legislations. Members **must** ensure records are both accurate and compliant with the respective Fraud Definitions. It is the responsibility of the Member who loaded a fraud record to delete or amend any records identified as having been incorrectly loaded by their Member organisation, and ensure records are kept up-to-date as the status of an investigation evolves. Data accuracy is of utmost importance and **must** form part of the loading review stage and User compliance check processes.

II.2.2. Guiding Principle

The success of the fraud data-sharing model relies on the integrity of the Data submitted, and it is imperative that Members maintain, update and delete records as appropriate to ensure that the highest standards of Data accuracy are adhered to.

II.2.3. Authorised Users Must:

- 11.2.3.1. Ensure all records are accurately populated, inclusive of the correct fraud status / outcome fields and (where applicable) NIM grading.
- 11.2.3.2. Amend, remove or update records of Confirmed and Suspect Fraud, as any new information in respect of the Data Subject(s) comes to light.

II.2.4. Authorised Users Must Not:

- 11.2.4.1. Leave records of Suspect Fraud in 'Under Investigation' status indefinitely. A final outcome status **must** be applied, (using the fraud status field), once this has been reached.
- 11.2.4.2. Unduly delay in removing or updating a record, where new information comes to light.

II.2.5. Interface Managers Must:

- 11.2.5.1. Assume responsibility within their Member organisation for ensuring that robust and appropriate policies are in place to ensure Data is deleted, amended and updated, as required.

II.2.6. Interface Managers Must Not:

- 11.2.6.1. Ignore, delay or postpone any communications or actions in respect of Data integrity requirements. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.



Automated weeding rules are in place across both Suspect and Confirmed Fraud, which will automatically remove records from the register once they have reached the maximum retention period for their record type, status and NIM rating. Intervention is only required in respect of interim record removals where a Data Subject challenges a loading or new information comes to light that changes or casts doubt on the outcome of the case.

Confirmed Fraud records can be hard deleted directly by the Member, both manually via the User interface and in bulk. Suspect Fraud records need to be set to 'Investigation Closed – No Fraud Found' to set the record to auto-delete after 48 hours. If a Suspect Fraud record needs to be immediately deleted, please contact the IFB to assist with this request.



II. LOADING – ACCURACY

II.2.7. Governance

- 11.2.7.1. Guidance on the requirement of accuracy and how to adhere to it will be made clear in annual compulsory training for the Confirmed and Suspect Fraud Data.
- 11.2.7.2. An acknowledgment of each Interface Manager's and Authorised User's responsibility to upholding the principle will be included in the annual attestation.
- 11.2.7.3. The IFB will ensure that processes within the Confirmed and Suspect Fraud Data encourage accuracy.

Accountability – All Authorised Users will be clear about their responsibilities to ensure the accuracy of the Data. The IFB will support Members through annual training so that all Authorised Users are trained to the same required standard.

Accessibility – Training and supporting documentation will be readily accessible online. Training and attestation will be issued on an annual basis by IFB. New Authorised Users will be allocated the training as part of their onboarding.

Transparency – As a prerequisite of obtaining access to the Confirmed and Suspect Fraud Data, Members must demonstrate an understanding of the need for accuracy via compulsory training. This approach will ensure all Members are confident that the same level of oversight exists across the industry.



12.

Complaints and DSARs

As a Data-driven industry utility, it is essential that the IFB and its Members remain fully compliant with Data protection legislation in respect of Data Subject rights under the UK Data Protection Act.

Industry interests in combatting fraud must be carefully weighed against Data Subject rights in respect of Confirmed or Suspect Fraud records loaded by the Member. A failure to observe Data Subject rights under the Act could result in reputational damage or adverse media exposure, which risks undermining collective confidence in the data-sharing model.



12. COMPLAINTS AND DSARS

12.1. COMPLAINTS AND DSARS

12.1.1. Safeguarding Data Subject Rights

- Yes
- Partial
- No
- N/A

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Transactional Data (CUE / MID / MIAFTR)	●	●	●
Suspect Fraud Data*	●	●	●
Confirmed Fraud Data*	●	●	●

* Subject to successful completion of due diligence.





12. COMPLAINTS AND DSARS

12.2. COMPLAINTS AND DSARS

Safeguarding Data Subject Rights

12.2.1. The IFB Complaints Policy

12.2.1.1. Stage One

- 12.2.1.1.1. A Data Subject obtains a copy of their Data held on the System(s) through submission of a Data Subject Access Request ('DSAR') to the IFB.

12.2.1.2. Stage Two

- 12.2.1.2.1. The Data Subject addresses their complaint to the Member.
- 12.2.1.2.2. The Member investigates the complaint in line with the timescales set out in the IFB Complaints Policy (as set out in Section 17.4 of this document), and reaches an outcome, amending or deleting the record as appropriate.
- 12.2.1.2.3. On completion of the investigation, the Member issues a 'final response' letter, in which the fraud finding is communicated explicitly to the Data Subject. The Member may also choose to explicitly reference the fact of subsequent loading to the Confirmed Fraud System.

12.2.1.3. Stage Three

- 12.2.1.3.1. Upon receipt of a complaint from a Data Subject, but only after a Member has issued their 'final response' letter, the IFB may investigate on appeal.
- 12.2.1.3.2. The IFB will ask the relevant Member for a copy of their evidence that the Fraud Definition has been met and the threshold for loading met.
- 12.2.1.3.3. The IFB will review the complaint within three Business Days and advise the Member and Data Subject of their decision, providing the contact details of the relevant bodies to which the Data Subject can escalate their complaint if they remain dissatisfied.

12.2.1.4. Notes

- 12.2.1.4.1. The above represents a summary only and **must not** be considered without reference to the complete IFB Complaints Policy (as set out in Section 17.4 of this document) and Data Disclosure requirements (as set out in Section 7 of this document).

- 12.2.1.4.2. The IFB also reserve the right to intervene in complaints which could attract media attention, are high-profile or could otherwise generate public interest.

- 12.2.1.4.3. The IFB reserves the right to act as adjudicator in the event of dispute between the Data Subject and loading party, and to compel the permanent removal of a Data Subject's details from the System(s), where the loading criteria have not been met in full.

12.2.2. Requirement

As a Data-driven industry utility, it is essential that the IFB and its Members remain fully compliant with Data protection legislation in respect of Data Subject rights. This includes observing and upholding the rights of Data Subjects under the UK Data Protection Act, including to challenge the loading of their Data.

12.2.3. Guiding Principle

Industry interests in combatting fraud **must** be carefully weighed against Data Subject rights in respect of Confirmed or Suspect Fraud records loaded by the Member. A failure to observe Data Subject rights under the Act could result in reputational damage or adverse media exposure, which risks undermining collective confidence in the data-sharing model.

12.2.4. Authorised Users Must:

- 12.2.4.1. In respect of DSARs and complaints:
- 12.2.4.2. Ensure familiarity with IFB DSAR and complaint handling requirements, as well as the IFB Data Disclosure requirements, as outlined in Section 7.
- 12.2.4.3. Be able to identify internal referral points for dealing with DSARs or complaints received, according to internal process.

12.2.5. Interface Managers Must:

In addition to the above, in respect of DSARs:

- 12.2.5.1. Only disclose Data held and used by the Member. This can include the Data held on the Data Subject as downloaded from the System(s). To note, Members are not required to actively search the System(s) for Data held on the Data Subject in order to satisfy the DSAR.
- 12.2.5.2. Instruct Data Subjects to make a DSAR to the IFB directly, if they require further information or wish to know which insurer uploaded their Data.
- 12.2.5.3. Notify the IFB of receipt of any DSAR which relates to IFB Data, inclusive of Confirmed or Suspect loadings made by the Membership.



12. COMPLAINTS AND DSARS

12.2.6. Interface Managers Must:

In respect of complaints:

- 12.2.6.1. Ensure close familiarity with IFB DSAR and complaint handling requirements, as well as the IFB Data Disclosure requirements (Section 7).
- 12.2.6.2. Ensure that all Data Subject complaints are acknowledged in writing within three Business Days and are responded to in full within one month.
- 12.2.6.3. Ensure that the IFB are notified of the fact and content of the complaint within three Business Days of receipt.
- 12.2.6.4. Ensure that the IFB are notified of final outcome to any complaint within three Business Days of closure.
- 12.2.6.5. Notify the IFB immediately in the event that a complaint risks resulting in media attention, is high-profile or could otherwise generate public interest.
- 12.2.6.6. Ensure any Data provided to the IFB in respect of any Data Subject complaint is sent securely via secure file share or password-protected zip file.
- 12.2.6.7. Comply with any reasonable directions given by the IFB in respect of such complaints provided, inclusive of removing a record where required.
- 12.2.6.8. Notify the IFB within three Business Days if the Information Commissioner, Ombudsman Service, other relevant body, a solicitor or court become involved in a complaint.

12.2.7. Interface Managers Must Not:

In respect of both DSARs and complaints:

- 12.2.7.1. Disclose information from the Data without a Data Subject having successfully completed a prior DSAR.
- 12.2.7.2. Send any Data provided to the IFB in respect of any Data Subject complaint via unsecured channels.
- 12.2.7.3. Disclose details of an intelligence loading, where this could prejudice an ongoing IFB or law enforcement investigation, in the event of disclosure.
- 12.2.7.4. Fail to action DSARs or complaints received in line with terms of the IFB Complaints Policy, Membership Rules and Membership Agreement.

12.2.8. Interface Managers Must:

In respect of DSARs, assume responsibility within their Member organisation for:

- 12.2.8.1. Implementing appropriate processes within the Member organisation to ensure DSAR handling and recording within relevant timescales.
- 12.2.8.2. Responding to DSARs which are received by the Member only in relation to the information that the Member holds. If Data has been accessed by the Member from the relevant System, this information can include such Data.
- 12.2.8.3. Providing the IFB with full cooperation and assistance in relation to any DSARs received.

In respect of complaints, assume responsibility within their Member organisation for:

- 12.2.8.4. Implementing appropriate processes to ensure that complaints are handled in line with the requirements of the IFB Complaints Policy, Membership Rules and Membership Agreement.
- 12.2.8.5. Submitting to the IFB on a monthly basis a summary of the total number and type of complaints received in respect of the relevant System(s).
- 12.2.8.6. Ensuring that any sub-contractor or other service provider whom it engages in connection with this Agreement shall implement defined and documented procedures to address Data protection-related complaints.
- 12.2.8.7. Co-operating fully in any defence of a claim against the IFB arising from the Member's use of the relevant Data.

12.2.9. Interface Managers Must Not:

- 12.2.9.1. Ignore, delay or postpone any communications or actions in respect of complaint handling, where these relate to IFB Data. Such action could result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to IFB Data, System(s) and services.



12. COMPLAINTS AND DSARS

12.2.10. Governance

- 12.2.10.1. An acknowledgment of the Interface Manager's responsibility to upholding the principle will be included in the annual attestation.
- 12.2.10.2. Interface Managers will be responsible for providing the IFB with evidence of a formal process to support the principle. This must be demonstrated annually.
- 12.2.10.3. IFB will provide a Complaints Process for Members to use (as set out in Section 17.4 of this document).

Accountability – Interface Managers will take responsibility for upholding the principle and ensuring appropriate processes are in place. The IFB will provide a Complaints Process for Members to use.

Accessibility – The Complaints Process will be clear and readily available to Members should it be necessary. Appropriate policies can be provided digitally to the IFB as part of onboarding, or as part of scheduled audit activity and / or on ad hoc request thereafter.

Transparency – This approach will ensure all Members are confident that the same level of oversight exists across the industry.



13.

Data Integrity

The Member is required to implement appropriate technical and organisational measures to minimise the risk of unauthorised use, loss or damage of the Data. Access to the System(s) must be limited to staff members who need it to perform their duties, with access levels appropriate to their roles. Audit trails must be maintained to capture who has accessed the System. Any Data Breaches involving Personal Data from the System(s) must be reported to the IFB within 24 hours of a Member becoming aware of the breach. Data must not be transferred outside the European Economic Area without prior written consent from the IFB.

The IFB data-sharing model is only as strong as the weakest link in the chain; Members have a collective responsibility for safeguarding the Data and ensuring that it is held securely at all times.



13. DATA INTEGRITY

13.1. DATA INTEGRITY

13.1.1. Ensuring Highest Standards of Data Protection and Information Security

- Yes
- Partial
- No
- N/A

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Transactional Data (CUE / MID / MIAFTR)	●	●	●
Suspect Fraud Data*	●	●	●
Confirmed Fraud Data*	●	●	●

* Subject to successful completion of due diligence.





13. DATA INTEGRITY

13.2. DATA INTEGRITY

Ensuring Highest Standards of Data Protection and Information Security

13.2.1. Requirement

The Member is required to implement appropriate technical and organisational measures to minimise the risk of unauthorised use, loss or damage of the Data. Access to the System(s) **must** be limited to staff Members who need it to perform their duties, with access levels appropriate to their roles. Audit trails **must** be maintained to capture who has accessed the System(s). Any Data Breaches involving Personal Data from the System(s) **must** be reported to the IFB within 24 hours of a Member becoming aware of the breach. Data **must not** be transferred outside the European Economic Area without prior written consent from the Board. Key examples of these requirements includes:

- 13.2.1.1. Members' Data security standards **must** be compliant with, or of a comparable standard to, ISO27001, which is assessed as part of a Member organisation's initial due diligence and on subsequent risk-based Member audit thereafter.
- 13.2.1.2. IFB Data **must** be kept confidential and handled in a manner that is appropriate for the sensitivity of Data.
- 13.2.1.3. Members **must** ensure IFB Data is not transferred outside the European Economic Area (EEA) without the prior written consent of the Board.
- 13.2.1.4. Members **must** report any instances of actual, suspected or threatened unauthorised disclosure, misappropriation, misuse, loss, corruption, damage to, deletion of, or Data Breach in respect of any of the Data within 24 hours of breach detection.
- 13.2.1.5. Members **must** ensure that Data is retained only for as long as is necessary to fulfil the Purpose (as set out in section 1.4) and take steps to routinely remove Data not meeting this criteria from internal systems and databases.
- 13.2.1.6. Formal Data-retention periods vary depending upon the status of the intelligence, grading of it (as graded by the National Intelligence Model methodology) and the risk deemed to be posed by the alleged fraud.
- 13.2.1.7. Access to the Data **must** be restricted to those staff that need it to do their jobs with an access level proportionate to the role being undertaken. Access **must not** be granted outside of a Member organisation's fraud or intelligence functions.
- 13.2.1.8. Members **must** use their best skills for regular and ongoing vetting of its staff appointed as the authorised personnel for the Member, or those allowed to use the IFB platform, responsible for uploading Data on the IFB platform, including vetting for the authorised personnel's fraud history.

13.2.2. Guiding Principle

The IFB data-sharing model is only as strong as the weakest link in the chain; Members have a collective responsibility for safeguarding the Data and ensuring that it is held securely at all times.

13.2.3. Authorised Users Must:

- 13.2.3.1. Ensure their login credentials are kept safe and secure.
- 13.2.3.2. Immediately report any instances of actual, suspected or threatened unauthorised disclosure, misappropriation, misuse, loss, corruption, damage to, deletion of, or Data Breach in respect of any of the Data. Interface Managers are obliged to report such instances directly to the IFB within 24 hours.
- 13.2.3.3. Only access the IFB Data and System(s) from within the permitted territory, which is the UK and EEA.

13.2.4. Authorised Users Must Not:

- 13.2.4.1. Share their login credentials with any other User under any circumstance.
- 13.2.4.2. Attempt to access IFB Data and System(s) from outside the permitted territory, which is the UK and EEA.
- 13.2.4.3. Attempt to circumvent these Rules and / or their Member organisation's internal information security protections, or attempt to share or send Data outside of the Member organisation. Any attempts of this nature are **strictly prohibited** and would constitute a breach of the Membership Rules and Membership Agreement, as well as a possible **criminal offence**.



13. DATA INTEGRITY

13.2.5. Interface Managers Must:

Assume responsibility within their organisation for:

- 13.2.5.1. Ensuring that all requirements in respect of Data protection and information security, as set out in the Membership Rules and Membership Agreement, are complied with in full.
- 13.2.5.2. Ensuring that no User access or access to the Data in bulk outputs are provided to parties who sit outside of the fraud or intelligence functions, or outside the UK or EEA.
- 13.2.5.3. Reporting any instances of actual, suspected or threatened unauthorised disclosure, misappropriation, misuse, loss, corruption, damage to, deletion of, or Data Breach in respect of any of the Data to the IFB within 24 hours.
- 13.2.5.4. Ensuring processes are in place to delete and refresh the Confirmed Fraud Data after seven days.

13.2.6. Interface Managers Must Not:

- 13.2.6.1. Ignore, delay or postpone any communications or actions in respect of Data integrity requirements. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.

13.2.7. Interface Managers Should:

- 13.2.7.1. In respect of Suspect Data, align their Data-retention limits to those of the IFB, as set out in Section 17.2 of this document.

	Status / File type	Retention Period		
		Crime Level 1	Crime Level 2	Crime Level 3
Suspect Fraud Data	Under Investigation	2 years	3 years	6 years
	Investigation closed – Confirmed Suspect	3 years	4 years	6 years
	Investigation closed – Confirmed Fraud*	30 days	30 days	30 days
	Investigation closed – Not Suspect	2 days	2 days	2 days
	Investigation closed – Victim	1 year	3 years	6 years
Transactional Data	MIAFTR	The earliest of 6 years after loss date or 6 years after creation date within the system		
	MID Policy Documents	Removed if they are closed and unchanged for 3 years		
	CUE Claims Records	3 years from the closure date or 6 years from the loss date or if neither are present 6 years from the notification date		
	Intelligence Feed	Full Data refresh conducted each day, previous Data deleted before new insertion		
Confirmed Fraud Data	All Confirmed Fraud records loaded	Auto-weeded 5 years from Create Date		

* This status is only set on closed suspect fraud submissions, once the record is moved to the Confirmed Fraud status, following a confirmed fraud finding.



13. DATA INTEGRITY

13.2.8. Governance

- 13.2.8.1. An acknowledgment of the Interface Manager's and Authorised User's responsibility to upholding the principle will be included in the annual attestation.
- 13.2.8.2. Interface Managers will be responsible for providing the IFB with evidence of a formal process to support the principle, which meets the standard set by ISO27001. This must be demonstrated annually.

Accountability – Interface Managers will take responsibility for upholding the principle and ensuring appropriate processes are in place.

Accessibility – The standard set by ISO27001 to ensure compliance is publicly available. Appropriate policies can be provided digitally to the IFB as part of onboarding, or as part of scheduled audit activity and / or on ad hoc request thereafter.

Transparency – As a prerequisite of obtaining Membership, Members must demonstrate suitable Data Integrity. This approach will ensure all Members are confident that the same level of oversight exists across the industry. Measures for Data Breaches are detailed in Section 16.



14.

Training and Compliance

A robust training and compliance provision is key in creating a secure data-sharing environment, where the Data is consistently managed, safeguarded, and aligned with the required IFB standards, the National Intelligence Model (NIM) and the UK Data Protection Act, thereby minimising the risk of errors and ensuring the Members meets their obligations under the Membership Agreement. The IFB is committed to carrying out compliance reviews of Member activity, which includes regular BAU compliance checks and risk-based audit visits as required.

Comprehensive training and compliance are cornerstones for engendering trust and compliance across the Member base, thereby driving collective confidence in the data-sharing model.



14. TRAINING AND COMPLIANCE

14.1. TRAINING AND COMPLIANCE

14.1.1. Ensuring User Awareness and Good Governance

- Yes
- Partial
- No
- N/A

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Role-based Attestation	●	●	●
NIM Training	●	●	●
Transactional Data (CUE / MID / MIAFTR)	●	●	●
Suspect Fraud Data*	●	●	●
Confirmed Fraud Data*	●	●	●

* Subject to successful completion of due diligence.





14. TRAINING AND COMPLIANCE

14.2. TRAINING AND COMPLIANCE

Ensuring User Awareness and Good Governance

14.2.1. Requirement

A robust training and compliance provision is key in creating a secure data-sharing environment, where the Data is consistently managed, safeguarded, and aligned with the required IFB standards, the National Intelligence Model (NIM) and the UK Data Protection Act, thereby minimising the risk of errors and ensuring the Members meets their obligations under the Membership Rules and Membership Agreement. The IFB is committed to carrying out compliance reviews of Member activity, which includes regular BAU compliance checks and risk-based audit visits as required.

14.2.2. Guiding Principle

Comprehensive training and compliance are cornerstones for engendering trust and compliance across the Member base, thereby driving collective confidence in the data-sharing model.

14.2.3. Authorised Users Must:

- 14.2.3.1. Undertake any training required by the IFB as both a precondition of initial access to System(s) and the Data, and as required by the IFB thereafter. This could include:
 - 14.2.3.1.1. User training days upon being nominated as an IFB User.
 - 14.2.3.1.2. E-learning training on IFB Data and System(s), functionality and compliance, the NIM model and other relevant subjects.
 - 14.2.3.1.3. Any other mandatory IFB Data and System(s) trainings or demos as required by the IFB from time to time.
- 14.2.3.2. Be aware that failure to complete training in the timescales required could result in individual suspension of access to IFB Data, System(s) and other services, and formal escalation to their Member organisation's Interface Manager and Head of Fraud.
- 14.2.3.3. Respond to any requests from their Member organisation's Interface Managers to support with compliance activity as required from time to time.

14.2.4. Authorised Users Should:

- 14.2.4.1. Attend or undertake any non-mandatory IFB training events or courses, as communicated by the IFB from IFB from time to time.

14.2.5. Authorised Users Must Not:

- 14.2.5.1. Ignore, delay or postpone any mandatory training, as issued by the IFB.

14.2.6. Interface Managers Must:

- 14.2.6.1. Assume responsibility within their Member organisation for ensuring collective compliance with IFB training requirements across their User base:
 - 14.2.6.1.1. Ensuring robust processes and procedures in place to ensure clear, adequate and regular internal training on IFB Data and System(s) is in place.
 - 14.2.6.1.2. Ensuring IFB Users regularly undertake internal Data protection, fraud awareness and information security training on an annual basis.
 - 14.2.6.1.3. Maintaining adequate records to indicate that Users have completed training and are competent to perform the required tasks.
 - 14.2.6.1.4. Ensuring that all nominated Users complete all IFB e-learning required in a timely manner.
 - 14.2.6.1.5. Responding to and actioning IFB communications highlighting outstanding User training activity in a timely manner.
- 14.2.6.2. Assume responsibility within their Member organisation for completing required IFB regular compliance checks. This includes:
 - 14.2.6.2.1. Ensuring compliance with regular dip sample requirements.
 - 14.2.6.2.2. In the event of a Member audit visit, providing the IFB with such information, cooperation, assistance and access to their premises during normal business hours. Per the Membership Agreement, the IFB shall conduct an audit after one calendar year from the date of Member sign-up, except where the IFB shall deem more frequent or earlier Member audits to be necessary, for example, in the event of a data breach.
 - 14.2.6.2.3. Conducting regular internal fraud file audits across both applications and claims as part of regular business-as-usual (BAU) activity.
 - 14.2.6.2.4. Ensure that any recommendations put forward as a result of an audit visit are appropriately actioned in timescales agreed with the IFB.



14. TRAINING AND COMPLIANCE

14.2.7. Interface Managers Must Not:

- 14.2.7.1. Ignore, delay or postpone any communications or actions in respect of IFB training and compliance requirements, as issued by the IFB. Such action may result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.

14.2.8. Interface Managers Should:

- 14.2.8.1. Attend or undertake any non-mandatory IFB training events or courses, as communicated by the IFB from time to time.
- 14.2.8.2. Proactively encourage their Authorised User base to attend or undertake any non-mandatory IFB training events or courses, as communicated by the IFB from time to time.

14.2.9. Interface Managers May:

- 14.2.9.1. Extend invites to IFB training events and courses to staff members within their organisation working outside fraud or intelligence teams, with prior approval from IFB. Completion of any training does not confer any associated privileges to IFB Data, System(s) or other services.

14.2.10. Governance

- 14.2.10.1. Interface Managers must assume responsibility for ensuring all mandatory training is undertaken and audit / compliance requirements completed.
- 14.2.10.2. The IFB will ensure all training, compliance and audit requirements are clearly communicated to Members.
- 14.2.10.3. Compliance processes will focus on ensuring compliance with Rules in regard to use of IFB System(s).

Accountability – Interface Managers will take responsibility to ensure appropriate training, compliance and audits are undertaken. The IFB will develop training, compliance and audit requirements which will support Members in complying with the Rules.

Accessibility – All training requirements and events will be clearly communicated to Members to ensure compliance. All compulsory training and compliance requirements will be consistent regardless of business size or book of business. All compulsory training and compliance requirements will be clear in how they support compliance with the Rules.

Transparency – Training and compliance requirements across Members will be the same to ensure confidence of compliance across the industry. Members failing to comply with training and compliance requirements may be subject to Measures as detailed in Section 16.



15.

Management Information

Ensuring collective participation in review and participation in Management Information (MI) is vital in providing actionable insights that support informed decision making, help track performance and support the identification of trends and modus operandi, thereby driving further value, insight and compliance across the Member base.

Members should exercise reasonable endeavours in collectively tracking and reporting financial benefits and savings from using the Data and System(s), recording the financial impacts related to fraud, and reporting complaints. Members should also make regular efforts to review Management Information (MI) to effectively monitor and manage transactional activity.



15. MANAGEMENT INFORMATION

15.1. MANAGEMENT INFORMATION

15.1.1. Leveraging MI for Benefits Mapping and Evidencing Compliance

- Yes
- Partial
- No
- N/A

1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
----------------------------	-----------------------------------	-----------------------

Transactional Data (CUE / MID / MIAFTR)	●	●	●
Intelligence / Feedback, etc. Submissions	●	●	●
Suspect Fraud Data*	●	●	●
Confirmed Fraud Data*	●	●	●





15. MANAGEMENT INFORMATION

15.2. MANAGEMENT INFORMATION

Leveraging MI for Benefits Mapping and Evidencing Compliance

15.2.1. Requirement

Members should exercise reasonable endeavours in collectively tracking and reporting financial benefits and savings from using the Data and System(s), recording the financial impacts related to fraud, and reporting complaints. Members should also make regular efforts to review Management Information (MI) to effectively monitor and manage transactional activity.

15.2.2. Guiding Principle

Ensuring collective participation in review and participation in MI is vital in providing actionable insights that support informed decision making, help track performance and support the identification of fraud trends and modus operandi, thereby driving further value, insight and compliance across the Member base.

15.2.3. Interface Managers Must:

- 15.2.3.1. Actively participate in Customer Relationship Management (CRM) meetings, to include a review and understanding of relevant MI detailing Member contribution across all key areas. The Interface Manager is responsible for ensuring that any gaps in reciprocity are communicated internally within the Member organisation, and a plan of action to increase contribution put into place.

15.2.4. Interface Managers Should:

- 15.2.4.1. On a reasonable endeavours basis, assume responsibility within their Member organisation for:
 - 15.2.4.1.1. Tracking and recording all benefits and financial savings that the Member derives from accessing and use of the relevant System(s) and Data.
 - 15.2.4.1.2. Analysing these benefits and reporting them back accurately to the IFB on a quarterly basis.
 - 15.2.4.1.3. Record any financial savings or losses attributed to each Confirmed or Suspect Fraud entered into the Systems(s).
 - 15.2.4.1.4. Submitting to the IFB on a monthly basis a summary of the total number and type of complaints received in respect of the relevant System(s).

- 15.2.4.1.5. Proactively reviewing, actioning and analysing their Member organisation's MI on Data and System(s) consumption, which is made available via a designated reporting interface, IFB-issued MI and through CRM meetings.

- 15.2.4.1.6. Actively reviewing MI issued by the IFB on a quarterly basis in respect of their organisation's activity, ensuring appropriate action is taken against dormant, inactive or no longer required Authorised Users.

15.2.5. Interface Managers Must Not:

- 15.2.5.1. Ignore, delay or postpone any communications or actions in respect of IFB MI requirements.
- 15.2.5.2. Fail to fulfil these obligations, as set out in the Membership Rules and Membership Agreement. Such action could result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.

15.2.6. Governance

- 15.2.6.1. MI submitted by a Member will be discussed at quarterly Customer Relationship Management (CRM) meetings, with a focus on how the IFB can deliver value, insight and compliance across the Member base.
- 15.2.6.2. MI issued by the IFB will be discussed at quarterly CRMs to ensure Members are monitoring Authorised User activity and deriving value from IFB Membership.

Accountability – Discussion between Members and the IFB on MI ensures a collaborative approach to driving further value, insight and compliance across the Member base.

Accessibility – Appropriate MI documents will be provided on a regular basis as set out in the Rules. Any raw data will be presented in a format that supports Members in undertaking further analysis to develop their value, insight and compliance.

Transparency – Having open discussions between Members and the IFB help promote good relationships and drive improvements.



16.

Compliance Support Framework

Ensuring Data accuracy and upholding standards is vital for the success and the integrity of the data-sharing model. Measures are available to address individual instances of persistent non-compliance, thereby safeguarding the integrity of the collective.

In the event of persistent or severe Data Breach, the IFB may recommend to the IFB Membership Committee that a sanction may be required to protect the integrity of Data held.



16. COMPLIANCE SUPPORT FRAMEWORK

16.1. COMPLIANCE SUPPORT FRAMEWORK

16.1.1. Ensuring Member Adherence through Compliance Support

- Yes
- Partial
- No
- N/A

	1 Full Member – Insurer	2 Full Member – Non Insurer	3 Community Member
Roles	●	●	●
Search	●	●	●
Contribution	●	●	●
Download	●	●	●
GDF	●	●	●
Feedback and Submissions	●	●	●
Data Disclosure	●	●	●
Data Protection and InfoSec	●	●	●
Complaints and DSARs	●	●	●



16.2. COMPLIANCE SUPPORT FRAMEWORK

Ensuring Member Adherence through Compliance Support

16.2.1. Requirement

It is imperative that Data held on the System(s) is accurate and correct, and that all Members are working to the required standards in respect of loading Data to the System(s) and safeguarding against Data Breaches in any form. In the event of persistent or severe Data Breach, the IFB **may** apply Measures to protect the integrity of Data held on the System(s).

16.2.2. Guiding Principle

Ensuring Data accuracy and upholding standards is vital for the success and the integrity of the data-sharing model. For this reason, Measures are available to address individual instances of persistent non-compliance, thereby safeguarding the integrity of the collective.

16.2.3. Authorised Users Must:

- 16.2.3.1. Adhere to all required standards as set out in the Membership Rules and the Membership Agreement.
- 16.2.3.2. Immediately report any instances of actual, suspected or threatened unauthorised disclosure, misappropriation, misuse, loss, corruption, damage to, deletion of, or Data Breach in respect of any of the Data to their designated Interface Manager and Head of Fraud.

16.2.4. Interface Managers and Heads of Fraud Must:

- 16.2.4.1. Be familiar with Section 16.1 and 16.2 of the Compliance Support Framework.
- 16.2.4.2. Handle and report any breaches of the Membership Rules, Membership Agreement and / or UK Data Protection Act, in accordance with the terms and conditions of the Membership Rules and Membership Agreement. This includes notifying the IFB of any loss of Data within 24 hours.
- 16.2.4.3. Agree an action plan with the IFB to ensure that sufficient controls are in place to ensure that further breaches of this policy will not take place. Following the completion of the agreed action plan the Member **may** make written representations to the IFB to reinstate full access to the Data.

16.2.5. Interface Managers and Heads of Fraud Must Not:

- 16.2.5.1. Ignore, delay or postpone any communications or actions in respect of Data Breach or Measures. Such action could result in formal escalation to their Member organisation's Head of Fraud and potential suspension of access to the IFB Data, System(s) and other services.

16.2.6. Governance

- 16.2.6.1. Acknowledgment of the Compliance Support framework will be required of all Roles in their annual attestation.
- 16.2.6.2. The Compliance Support framework will focus on the principles outlined in the Rules, what constitutes a breach and any Measure required to mitigate risks to Members and IFB.
- 16.2.6.3. Breaches will be scored on a quarterly basis and reported as part of Customer Relationship Meetings (CRM). IFB will work with Members to help prevent future breaches and improve compliance. Where there have been significant breaches to the Rules a Member will be referred to the Membership Committee for consideration of possible sanctions.

Accountability – All roles take responsibility for understanding the Compliance Support framework .

Accessibility – The Compliance Support framework will be made readily available to all roles and presented in clear language. Roles and responsibilities and IFB training will support all roles in understanding the relevance of the Compliance Support framework.

Transparency – The Membership Committee will provide oversight of any potential sanctions to be applied to Members. Any decision to permanently suspend a member must be ratified by the IFB Board.



16. COMPLIANCE SUPPORT FRAMEWORK

16.2.7. Introduction

The Compliance Support and Measures framework has been developed to support a collaborative approach between Members and IFB to work towards good Governance, maintain confidence in the integrity of IFB Data and all Members use of IFB products and services.

16.2.8. How the framework operates

Detailed in section 16.1 are a number of events which represent a failure to uphold **Must / Must Not** obligations detailed in the Rules, which pose a potential risk or cause actual harm to the wider Membership and IFB. Each event comes with a corresponding support and / or measure that seeks to mitigate any associated risk / harm and prevent the event happening in the future.

The support and / or measures specified seek to provide a resolution to specific events and do not represent long term restrictions to IFB services to Members.

To ensure ongoing compliance across the Membership, each event is scored based upon its risk of harm to the Membership and IFB, as detailed in Section 16.2. On a quarterly basis, these scores will be tallied to produce a Quarterly Compliance Score and reported as part of quarterly CRMs. The matrix in Section 16.2 sets out the details of actions that must be undertaken by a Member and IFB, depending upon the Quarterly Compliance Score.

Any actions that are applied will seek to ensure the Members and IFB work together towards ongoing compliance with the Rules and provide opportunities to identify improved ways of working. Only where a Member poses an immediate and significant risk to the Membership and IFB based upon their Quarterly Compliance Score will they be referred to the Membership Committee and IFB products and services potentially suspended.

16.2.9. Event Support and Measures Risk Scoring Matrix

Principle	Event	Support/Measure	Risk Score
Roles & Responsibilities	User fails to adhere to roles and responsibilities set out in the Rules	Refresher training on Roles and Responsibilities Escalation to Interface Manager	1
Confirmed Fraud Data; Data Disclosure; Threshold Complaints and DSARs; Transparency	Failure to demonstrate appropriate policies are in place within 20 Business Days of deadline	Suspension of relevant products until this can be demonstrated	2



16. COMPLIANCE SUPPORT FRAMEWORK

Principle	Event	Support/Measure	Risk Score
Search	User scores Amber in Transaction Data search compliance check	Refresher training for the User User subject to a compliance check within one month	1
	User scores Amber in Transaction Data search compliance check on two consecutive occasions	Internal Member review of staff member User subject to a compliance check within one month	2
	User scores Red in Transaction Data search compliance check	User account suspended. The account will not be reinstated until training has been completed	3
	User scores Red in Transaction Data search compliance check on two occasions within a 12-month period	User account suspended. Review of Roles and Responsibilities and User training needs with Interface Manager Plan agreed between Interface Manager and IFB to work toward reinstatement of User account	4
	User undertakes search on behalf of, or under instruction from any party not an existing Member of the IFB	User account suspended. Review of Roles and Responsibilities and User training needs with Interface Manager Plan agreed between Interface Manager and IFB to work toward reinstatement of User account	5
Generic Data Feed	Users uses or accesses the Generic Data Feed on behalf of any party not an existing Member of the IFB	User access to the Generic Data Feed file to be restricted by Interface Manager. Review of Roles and Responsibilities and User training needs with Interface Manager Plan agreed between Interface Manager and IFB to work toward reinstatement of User access to the Generic Data Feed	5
Confirmed Fraud Data	Users uses or accesses the Confirmed Fraud Data on behalf of any party not an existing Member of the IFB	User access to Confirmed Fraud Data file to be restricted by Interface Manager. Review of Roles and Responsibilities and User training needs with Interface Manager Plan agreed between Interface Manager and IFB to work toward reinstatement of User access to the Confirmed Fraud Data	5



16. COMPLIANCE SUPPORT FRAMEWORK

Principle	Event	Support/Measure	Risk Score
Data Disclosure; Complaints and DSARs	User discloses IFB intelligence contrary to NIM handling instructions	Refresher training for User responsible for breach Internal Member review to ensure all staff members are appropriately trained	3
	User discloses IFB Data contrary to DPA	Review(s) between Interface Manager and IFB within five Business Days of the breach to understand full extent of breach and potential risk to Members and IFB. If necessary, a plan will be implemented by IFB to mitigate the risk to other Members and IFB	5
Threshold	Two non-compliant records loaded within a six – month period	Refresher training for all Users with loading privileges	2
	Three or more non-compliant records loading within a 6-month period	Review of two-person review process to be undertaken between Interface Manager and IFB	3
Complaints and DSARs	Failure to adhere to IFB Complaints Policy and / or Complaints and DSARs Rules	Review of Member complaints procedure between Interface Manager and IFB	3
Data Integrity	IFB Data is transferred outside of the UK or EEA (without IFB approval)	Review(s) between Interface Manager and IFB within five Business Days of the breach to understand full extent of breach and potential risk to Members and IFB. If necessary, a plan will be implemented by IFB to mitigate the risk to other Members and IFB	5
Training and compliance	User does not complete compulsory training within deadline	Escalation to Interface Manager	1
	User does not complete compulsory training within ten Business Days of deadline	Escalation to Head of Fraud	1
	User does not complete compulsory training within 20 Business Days of deadline	Relevant accounts suspended until training complete	2



16. COMPLIANCE SUPPORT FRAMEWORK

Principle	Event	Support/Measure	Risk Score
Automated Decision Making	Failure to notify IFB of intention to automate decision making	Suspension of access to Confirmed Fraud Data pending attestation from the Head of Fraud that the decision making process meets the criteria set out in the Rules	3
	Applying automated decision making to Data other than the Confirmed Fraud Data	Suspension of access to the Data pending confirmation from the Head of Fraud that the automated decision making using Data other than the Confirmed Fraud Data has ceased	5
	Applying automated decision making using the Confirmed Fraud Data for non-fraud purposes	Suspension of access to the Confirmed Fraud Data pending confirmation from the Head of Fraud that the automated decision making for non-fraud purposes has ceased	5

16.3. QUARTERLY COMPLIANCE SCORE MATRIX

16.3.1. How the Quarterly Compliance Score is calculated

16.3.1.1. Each event detailed above is given a compliance score corresponding to the potential risk or harm to Members and IFB. On a quarterly basis, a Member's compliance score will be tallied to provide a Quarterly Compliance Score, with a corresponding action to be undertaken by Members and IFB. The scoring has been weighted to place an onus on Members and IFB collaborating to resolve any breaches and take steps to improve compliance. Only where there

is significant failure to comply with the Rules would a Member referred to the Membership Committee for consideration of potential sanctions, which could include the suspension of products and services. In the extreme situation where a Member presents an immediate and significant risk to the Membership and IFB, access to IFB products and services may be temporarily suspended at the discretion of the IFB Director.

16.3.1.2. Where an event precedes another event, for example, a User fails to complete training with ten Business Days AND 20 Business Days of the deadline, then the highest risk score will be taken. Following the conclusion of a quarter, a Member's Quarterly Compliance Score will be reset to zero.



16. COMPLIANCE SUPPORT FRAMEWORK

Event Risk Score	Compliance Score
1 (Very Low – User breach with no damage to Membership / IFB)	2
2 (Low – Minor Member / User breach which can be managed with immediate action. Low/no damage to Membership / IFB)	4
3 (Medium – Significant User breach which poses risk of damage to Membership / IFB which can be managed with immediate action. Member breach indicative of poor compliance but low/ no damage to Membership / IFB)	8
4 (High – Significant User breach which causes damage to Membership / IFB. Member breach which poses risk of damage to Membership / IFB)	16
5 (Very High – Significant Member breach which causes damage to Membership / IFB)	32

Quarterly Compliance Score (QCS)	Member and IFB Action
QCS <=8	Relevant events to be raised at quarterly Customer Relationship Meeting (CRM), but no further action by Member required.
8 < QCS <=32	Relevant events to be discussed at quarterly CRM and update provided by Interface Manager on action taken.
32 < QCS <=64	Member to undertake self audit of IFB services subject to a breach of the Rules over the quarter. Interface Manager to feedback at next CRM on action taken to improve compliance
QCS >64	IFB to present report on breaches to the Membership Committee who will recommend appropriate sanctions In the extreme situation where a Member presents an immediate and significant risk to the Membership and IFB, access to IFB products and services may be temporarily suspended at the discretion of the IFB Director.



17.

Appendix





17.1. FRAUD DEFINITIONS

17.1.1. Confirmed Fraud Definition

For the purposes of the IFR and this Agreement only, 'Fraud' shall be considered to have taken place in any circumstances where:

- any party seeking to obtain a benefit under the terms of any insurance related product, service or activity can be shown, on a balance of probabilities, through its actions, to have made or attempted to make a gain or induced or attempted to induce a loss by intentionally and dishonestly:
 - a. making a false representation; and / or
 - b. failing to disclose information; and / or having abused the relevant party's position.

and

- one or more if the following outcomes has taken place which relates to the fraudulent act:
 - c. an insurance policy application has been refused; and / or
 - d. an insurance policy or contract has been voided, terminated or cancelled; and / or
 - e. a claim under an insurance policy has been repudiated (whether in full, head, letter or part of such a claim); and / or
 - f. a successful prosecution for fraud, the tort of deceit or contempt of court has been brought; and / or
 - g. the relevant party has formally accepted his/her guilt in relation to the fraudulent act in question including, but not limited to, accepting a police caution; and / or
 - h. an Insurer has terminated a contract or a non-contracted relationship/recognition with a supplier or provider; and / or

- i. an Insurer has attempted to stop/recover or refused a payment(s) made in relation to a transaction; and / or
- j. an Insurer has challenged or demonstrated that a change to standing policy Data was made without the relevant customer's authority

17.1.2. Provided that...

The relevant party has been notified that its claim has been repudiated, or relevant policy or contract voided, terminated, or cancelled, for reasons of fraud and / or it is in breach of the relevant terms and conditions relating to fraud within the relevant policy or contract.

For the purposes of the IFiHUB and of this Agreement, 'Fraud' shall be considered to be present where a party is, or there are reasonable grounds to believe that a party seeking to obtain, or has obtained, a benefit under the terms of any insurance related product, service or activity by intentionally and dishonestly:

- a. making a false representation; and / or
- b. failing to disclose information; and / or
- c. having abused their position.

17.2. DATA RETENTION

17.2.1. IFB Data-Retention Periods

The IFB receives and generates significant quantities of intelligence from a number of sources, which include personal and special category Data.

In order to maintain compliance with Data protection and other relevant legislation, the IFB ensures that Data is processed ethically and for the permitted purpose only. Data is retained only for as long as is necessary to fulfil its purpose, and Data not meeting this criteria is routinely removed from

systems and databases. Formal Data-retention periods vary depending upon the status of the intelligence, grading of it (as graded by the National Intelligence Model methodology) and the risk deemed to be posed by the alleged fraud.

All processing of Data by the IFB is restricted to the purpose of detecting and preventing insurance fraud. IFB Members are expected to adhere to equivalent standards as set out above which comply with the relevant legislation.

	Status / File type	Retention Period		
		Crime Level 1	Crime Level 2	Crime Level 3
Suspect Fraud Data	Under Investigation	2 years	3 years	6 years
	Investigation closed – Confirmed Suspect	3 years	4 years	6 years
	Investigation closed – Confirmed Fraud*	30 days	30 days	30 days
	Investigation closed – Not Suspect	2 days	2 days	2 days
	Investigation closed – Victim	1 year	3 years	6 years
Transactional Data	MIAFTR	The earliest of 6 years after loss date or 6 years after creation date within the system		
	MID Policy Documents	Removed if they are closed and unchanged for 3 years		
	CUE Claims Records	3 years from the closure date or 6 years from the loss date or if neither are present 6 years from the notification date		
	Intelligence Feed	Full Data refresh conducted each day		
Confirmed Fraud Data	All Confirmed Fraud records loaded	Auto-weeded 5 years from Create Date		

* This status is only set on closed suspect fraud submissions, once the record is moved to the Confirmed Fraud status, following a confirmed fraud finding.



17.3. NATIONAL INTELLIGENCE MODEL (NIM) GRADING

17.3.1. Source Evaluation

The evaluation of the source credibility helps inform how the intelligence might be used tactically.

1 – Reliable	The grading is used when there are no reasonable grounds to doubt the reliability of the source; the source is believed to be competent and information received is generally reliable. This may include information from human intelligence, technical, scientific and forensic sources
2 – Untested	This relates to a source that has not previously provided information to the person receiving it or has provided information that has not been substantiated. The source may not necessarily be unreliable, but the information provided should be treated with caution. Before acting on this information corroboration, should be considered. This would apply to information when the source is anonymous such as CheatLine or Crimestoppers report.
3 – Unreliable	This should be used where there are reasonable grounds to doubt the reliability of the source. This may include concerns regarding the authenticity, trustworthiness, competence or motive of the source or confidence in the technical equipment. Before acting on this information, corroboration should be sought.



17.3.2. Intelligence Reliability

This grading helps assess the reliability of the intelligence based upon how the source obtained it and what other intelligence might be available.

Where the intelligence cannot be corroborated, consideration should be given to what further research might be undertaken to corroborate it.

A – Known directly to the source	Refers to information obtained first-hand, e.g. through witnessing it. Care must be taken to differentiate between what a source witnessed themselves and what a source has been told or heard from a third party.
B – Known indirectly to the source but corroborated	Refers to information that the source has not witnessed themselves, but the reliability can be corroborated by other information. This corroboration could come from technical, other intelligence, investigations or enquiries. Care should be taken to ensure that the information that is presented as corroboration is independent and not from the same origin.
C – Known indirectly to the source	Applies to information that the source has been told by someone else. The source does not have first-hand knowledge of the information as they did not witness it themselves, e.g. where a person has been told by a friend of concerns about the activity of a firm of solicitors.
D – Not Known	This applies where there is no means of assessing the information. This may include information from an anonymous source, or partners such as CheatLine. This grade should only be used when it is genuinely not known how the source came to know the information.
E – Suspected to be false	Regardless of how the source came upon this information, there is a reason to believe the information provided is false. Where this is the case, the rationale for why it is believed to be false should be documented in the intelligence report.



17. APPENDIX

17.3.3. Intelligence Confidence Matrix

The Intelligence Confidence Matrix provides an indication of the level of confidence that can be taken in intelligence. This helps inform decision making and deciding what action may be taken.

	Reliable (1)	Untested (2)	Unreliable (3)
Known indirectly to the source but corroborated (B)	High	High	Medium
Known directly to source (A)	High	Medium	Low
Known indirectly to the source (C)	Medium	Medium	Low
Not known (D)	Low	Low	Low
Suspected to be false (E)	Low	Low	Low

17.3.4. Handling Codes

Handling codes provide a mechanism for intelligence sharing.

This includes handling conditions for providing additional information.

Those looking to disseminate intelligence should also ensure they are familiar with any other legislation, policies or procedures which might influence the sharing of intelligence.

P – Lawful sharing is permitted	In order to share this intelligence there must be: a fraud prevention or detection purpose, local protocols in place and a legitimate need to receive it.
C – Lawful sharing is permitted with conditions	This code permits dissemination but requires the receiving organisation to observe conditions as specified. Application of this code means the report author has applied specific handling instructions in respect of this information. Handling conditions will be contained within the appropriate Section of the intelligence report and the recipient must abide by these. If the recipient wishes to conduct further activities outside of the conditions then contact must first be made with the report author.



17. APPENDIX

17.3.5. Action and Sanitisation Codes

Where a handling code 'C' is applied, action and sanitisation codes must also be added to the report.

These codes provide instructions on what the recipient is allowed to do with the intelligence, both in terms of further sanitisation and action.

Additional comments can also be added to the report to make clear any handling instructions.

As standard, IFB Intelligence Reports are coded A2-S2 – Covert use-Consult originator.

Authorisation should be sought from the author before an IFB Intelligence Report is disseminated further.

Required Action	
A1 – Covert Development	Intelligence may be combined or corroborated with other intelligence but action cannot be taken directly. Permission must be sought from the originator before action is taken or the intelligence is shared further.
A2 – Covert Use	Action may be taken on this intelligence although the source, technique and any wider investigative effectiveness must be protected. This intelligence may not be used in isolation as evidence, to support repudiation or be referenced in litigation proceedings.
A3 – Overt Use	Overt action is permitted on this intelligence. This information can be used for specific details required by report author.
Sanitisation	
S1 – Delegated Authority	The report author of the intelligence permits the unsupervised sharing and sanitisation of the material in order to allow dissemination to the recipient's suppliers.
S2 – Consult Originator	The report author of the intelligence does not permit the sharing or sanitisation of the material for wider dissemination without permission.

17.3.6. Crime Levels

Crime levels are used to describe the extent of the criminality detailed within the intelligence. These have been adapted by IFB to reflect the nature of insurance fraud. The table below explains what each of the three levels represents.

Level 1	Local – (Believed) only 1 insurer affected
Level 2	Cross border – (Believed) more than one insurer affected
Level 3	Serious and Organised (Believed) A significant number of insurers affected



17.4. IFB COMPLAINTS POLICY

17.4.1. Responsibilities

The following roles need to be familiar with and understand these instructions:

- Post Room
- Head of Risk and Compliance
- Customer Relationship Manager
- MIB Customer Service and complaints Manager
- IFB Service Delivery Manager
- Product Manager
- System Support Specialist
- IFB Director
- Insurer Members (Relevant Insurance Company)
- Insurer Record and Member Administrators (Relevant Insurance Company)
- Insurer Executive complaints Team (Relevant Insurance Company)

All the roles identified above will be involved in the identification, escalation and / or the appropriate management of complaints.

17.4.2. Introduction

The System holds the details of individuals who have committed or are suspected of committing insurance fraud. Insurers can load fraud details onto the system and can search against records of suspect and confirmed fraud.

This document sets out the independent process to manage customer complaints about the system or Data loaded on to the system in an impartial manner.

17.4.3. How is a complaint defined?

Whilst the IFB is not regulated by the Financial Conduct Authority (FCA), all insurers are. Therefore, the complaints received by insurers and by the IFB regarding the system will be defined and processed as far as possible in accordance with the FCA handbook definition, which is:

- “Any oral or written expression of dissatisfaction, whether justified or not, from, or on behalf of, a person about the provision of, or failure to provide, a financial service or a redress determination, which:
 - alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience; and
 - relates to an activity of that respondent, or of any other respondent with whom that respondent has some connection in marketing or providing financial services or products, which comes under the jurisdiction of the Financial Ombudsman Service.”

17.4.4. Receiving the complaint

Complaints can be received through any medium. All written correspondence should be date stamped.

The complaint should be forwarded to the Product Manager at the IFB who will coordinate further action. This may involve referring the complaint to the Interface Manager within the insurer for further action.

If the complaint is received by the insurer, it will fall within the insurer’s own complaints process unless the insurer believes that the complaint ought to be considered by the IFB, in which case it should be forwarded immediately to supportcenter@insurancefraudbureau.org.



17. APPENDIX

17.4.5. Service Level

All complaints will be acknowledged within three Business Days and will be responded to in full within one month from receipt of the complaint. However, the IFB and the Member should make every effort to respond in full, as quickly as possible and in accordance with the timescales set out in the complaints Guide below.

17.4.6. Who should investigate and respond to complaints relating to Data loaded to the system?

Complaints relating to Data held on the system should be dealt with by the insurer who loaded the record in the first instance. If a consumer is made aware that their information is held on the system but does not know which insurer loaded them, they should be directed towards the Data Subject Access Request (DSAR) process, as detailed within the FAQ Section of the IFR website at www.theifr.org.uk (in respect of Confirmed Fraud Data only).

Examples of complaints relating to the system which should be handled by the insurer are:

- Data Subject receives insurer notification that their details will be loaded onto the system (in respect of Confirmed Fraud only).
- Data Subject attempts to purchase a new policy or receives a policy renewal notice and discovers their details are held on the system (in respect of Confirmed Fraud)
- Data Subject was unaware that their details had been placed on the System.
- Data Subject notified that details are on the system following a DSAR.
- In certain circumstances, the IFB may be responsible for investigating and handling the complaint. Examples of such complaints are as follows:
- Data Subject advises that Data on the system is inaccurate or incorrectly loaded and is being disputed with the loading insurer.
- Data Subject believes details loaded in error as a result of incorrect identification.

The above lists are not exhaustive. If an insurer receives a complaint and is unsure whether to deal with the complaint themselves or pass it to the IFB to consider, they should contact the IFB at supportcenter@insurancefraudbureau.org.

17.4.7. Complaints attracting media attention or public interest

Any complaint that is received by the IFB meeting the following criteria must be notified to the Communications Department and Product Manager of the IFB:

- The complainant has threatened to go to the media.
- The complainant has gone to the media.
- The issue has already received or is likely to receive media attention.
- The issue has or could have public interest.
- If IFB's reputation could or has received adverse attention.

In any of the above circumstances the Communications Department, Product Manager, Service Delivery Manager, and IFB Director must agree a way forward, who responds and how the IFB responds. The Director will agree referral to the Chair of the IFB Supervisory Board where appropriate.

If a complaint is received by the insurer which meets the above criteria, the insurer must notify the Product Manager of the IFB at supportcenter@insurancefraudbureau.org upon receipt of the complaint. The Product Manager will communicate what further steps are required.

17.4.8. High-profile complaints

Communication from government representatives or MPs, or addressed to the IFB Director or IFB Board Member, received by an insurer, must immediately be notified to the Product Manager at supportcenter@insurancefraudbureau.org, who will notify the IFB Director. If received by any part of the IFB, the complaint must immediately be passed to the Product Manager who will pass a copy to the IFB Director. Any high-profile complaint will require a response or authorised response from the IFB Director. The Product Manager will co-ordinate the investigation and ensure the complaint is responded to within the FCA response deadline.



17.4.9. Insurer complaints process

Upon receipt of a complaint regarding the system via any medium, the insurer will provide the complainant with a prompt written acknowledgement. If the complaint needs to be passed to the IFB (in accordance with Sections 6, 7 or 8 of this document), the insurer must advise the complainant that the matter is being referred to the IFB and provide the IFB contact details below:

Product Manager
Insurance Fraud Bureau
Linford Wood House
6-12 Capital Drive
Linford Wood
Milton Keynes
MK14 6XT

If the insurer is required to investigate and respond to the complaint themselves, the insurer will address the complaint within their own complaints procedure and in accordance with FCA Guidelines.

If the insurer Member is unsure whether the complaint should be investigated by the insurer or the IFB, such queries should be referred to supportcenter@insurancefraudbureau.org.

If the insurer receives the complaint via telephone and it is required to be passed to the IFB, the insurer will request that the consumer directs their complaint in writing to the above address, or by email to supportcenter@insurancefraudbureau.org.

Insurers must advise the complainant of their rights to appeal to the Financial Ombudsman Service if they are unhappy with the final response received. Insurers must send details of all complaints received to IFB on a monthly basis in accordance with Section 12 of this document.

17.5. IFB COMPLAINTS POLICY

17.5.1. Acknowledgment of the complaint

On receipt of a complaint to the IFB, the IFB will check whether the Data Subject is on the system, and will acknowledge the complaint within three Business Days by sending a holding letter or email to the customer, depending on the customer's method of communication. This must:

- Acknowledge the complaint.
- Apologise for the fact that the complainant felt cause to complain.
- Direct the customer towards the DSAR process, where applicable.
- Provide timescales for further response.

The complaint will be allocated as an open ticket in the IFB's workflow management system.

Should the complaint be deemed complaint in need of further escalation, the complaint handler will notify the Product Manager and IFB Service Delivery Manager in the first instance.

Within three Business Days, the IFB will send details of the complaint to the insurer. If the complaint would be most appropriately handled and responded to by the insurer, the IFB will send the complaint to the Interface Manager at the insurer, referencing the system record ID (as opposed to live Data) and requesting a copy of the letter notification issued to the Data Subject prior to Confirmed Fraud loading via a secure channel (in respect of Confirmed Fraud Data only).

Within the customer acknowledgement, the IFB will include confirmation that the matter has been passed to the insurer along with their contact details.

The IFB will maintain a record of the complaint via the complaints Log, as well as retaining copies of complaint correspondence.



17. APPENDIX

17.5.2. Investigation

If the IFB retain the complaint and require a response from the insurer, IFB will notify the Interface Manager at the insurer. The insurer will investigate the complaint and respond to the IFB within one month, giving the insurer's decision and reasons for that.

In instances of challenging or complex cases, the IFB may also seek to schedule a meeting with the loading party to discuss the circumstances of the loading, and may also request a copy of the full case notes via a secure channel. The IFB will review complaints from a position of impartiality, with reference to the respective Fraud Definition.

The IFB may also seek internal advice from the below key contacts within the organisation:

- The IFB Director
- Senior Compliance Officer, Privacy Team
- MIB Customer Service and Complaints Manager,
- Legal Counsel, Finance

If the IFB disagrees with the insurer's decision, the Product Manager will contact the insurer prior to issuing any response. If an agreement cannot be reached, the Product Manager will decide whether the case should remain on the system.

The IFB will issue a final written response to the complainant within three Business Days following receipt of the complaint. The complaint response must include:

- An acknowledgement of the specific complaint(s) issue(s) raised.
- Explanation of the IFB's decision (whether complaint accepted or not).
- Details of any further information required (if necessary).
- Details of the Financial Ombudsman Service should the complainant not agree with the decision.
- Advice that the complainant may refer the matter directly to the court.
- Advise customer they are entitled to seek independent legal advice to assist them if they wish, alternatively they can seek advice from their local branch of the Citizens Advice Bureau.

17.5.3. Removal of Records

Complaints should be responded to within one month of receipt. In complex cases, it is acknowledged that the one-month timescale may be exceeded. In such instances, the Data Subject should be provided with a holding response explaining why there is a delay, what steps are being taken to resolve the complaint, and when the Data Subject can expect a resolution.

If, following investigation of the complaint, a record is required to be removed from the system, the Interface Manager at the loading insurer will be notified by IFB immediately of this decision. The Interface Manager will be responsible for removing the record from the system within three Business Days of being notified.

17.5.4. Management Information

Insurers will send a complaints report for the previous month to the Product Manager by the seventh working day of each month. This report should include:

- Volume of complaints received.
- Details of resolved complaints.
- Details of outstanding complaints.
- Analysis on the nature of the complaints.

At the start of each quarter the Product Manager will issue a report of the previous quarter's complaints in summary format, highlighting trends. The report will be reviewed to identify any requirements for improvement in service.


QUESTIONS

supportcenter@insurancefraudbureau.org

Contact us

To find out more about the IFB please contact:
info@insurancefraudbureau.org

Linford Wood House, 6-12 Capital Drive,
Milton Keynes, MK14 6XT

 [insurancefraudbureau.org](https://www.insurancefraudbureau.org)



[@insurancefraudbureau939](https://www.youtube.com/channel/UC...)



[Insurance Fraud Bureau](https://www.linkedin.com/company/insurance-fraud-bureau)



[Insurancefraudbureau](https://www.instagram.com/insurancefraudbureau)



[Insurance Fraud Bureau](https://www.facebook.com/insurancefraudbureau)