UK Multi-Network IoT SIM Codes of Practice

Introduction

Fraud is a major concern in the telecommunications industry and BT is subject to attack by fraudsters who attempt to acquire Network services by deception and with intent to avoid payment. The decision by Us to sell services to You will mean that We must share the responsibility for combating fraud. This Code of Practice has been prepared to minimise fraudulent activities related to Our Network and You. The Code entails the actions carried out by Us and You or Your Resellers, End-Users and Users.

Two classifications of clauses are detailed and will be preceded by **M** meaning Mandatory and **A** meaning Advisory. This Code of Practice may be revised from time to time by Us and in urgent cases may be supplemented with a process, which will be emailed to You for immediate action.

1. Definitions

In this Code of Practice the following additional definitions will apply in this Schedule:

Activate	Change to a Subscription's state to allow Connection to the Network
Deactivate	Change to a Subscription's state to prevent Connection to the Network
Reactivate	Change of Subscription state to Activated following a period of Deactivation
Retired	State which does not allow Connection where the intention is that the Subscription will not be used again
Purge	Permanent removal of a Subscription from the Network

2. Lost, Stolen and Fraud management

M2.1 We have provided You with access to the IoT SIM management platform which is a self-service platform which allows you to Activate, Deactivate and Reactivate Subscriptions. It is your responsibility to Deactivate any Subscriptions that are lost/stolen or You suspect have been used fraudulently. You are liable for Usage Charges incurred until the point at which You Deactivate a Subscription.

If You determine that a Subscription will not be required in future (due to it being lost/stolen/used fraudulently), You must let us know. Termination Fees may apply – please check the UK Multi-Network IoT SIM Order Form.

3. Responsibilities

3.1 Our Responsibilities

M3.1.1 We and any subcontracted third parties who we engage to supply the service will assume the responsibility for the creation and maintenance of the Network and SIM management platform which are as far as reasonably practicable, resilient to fraud. We will inform You as soon as reasonably practicable where We are aware of apparent fraudulent use of the Network.

We and our subcontracted third parties monitor all network activity for evidence of fraud and/or abuse, including (but not limited to) Voice, Text and Data usage.

3.2 Your Responsibilities

M3.2.1

The IoT SIM management platform provides You with the autonomy to control your Subscriptions which You assume responsibility for. You must assume the responsibility of exercising care and good security practices when Activating and Deactivating Subscriptions on the Network.

M3.2.2 You assume full financial responsibility for Your Resellers, End-Users and Users, including credit checking, billing and payment collection.

M3.2.3 Any suspicions of fraud must be reported to the BT IoT/M2M Support Team immediately (within 1 hour) from detection. You are liable for Usage Charges incurred until the point at which You Deactivate the Subscription.

4. Your Resellers, End-Users and Users

M4.1 You shall assume full responsibility (including all financial liability) for Your Resellers, End-Users and Users usage of the Services and the IoT SIM Management Platform which We supply to You.

5. Fraud Action

M5.1 If We suspect fraudulent activity regarding Your Subscriptions We shall notify You.

M5.2 We reserve the right to suspend a Subscription's Connection to the Network if We suspect fraudulent activity. We shall notify You of the suspension. It is Your responsibility to notify the Reseller, End-User or User of the suspension. In the event of a Reseller, End-User or User contacting Us directly We will refer them to You.

6. High Usage Profiling

M6.1 We and our subcontracted third parties monitor Subscriptions on the Network for excessive Voice and SMS usage. If We notify You of excessive usage, it is Your responsibility to take appropriate action and bear the full financial liability of debts incurred.

7. Disconnecting from the Network

M7.1 You may request a Subscription is Disconnected from the Network at any time (In accordance with the UK Multi-Network IoT SIM Service Agreement including Termination Fees). Once We have Purged a Subscription from the Network, it is not possible to Reconnect that Subscription.

8. Sale of SIM Cards

M8.1 You are not permitted to sell SIM Cards to Resellers, End-Users or Users without an associated Subscription. This is to prevent large numbers of uncontrolled SIM Cards entering into the market and being used in the future with stolen/cloned equipment.

9. Access to the IoT SIM Management Platform

A9.1 BT provides secure access to the IoT SIM Management Platform and APIs.
Access to the API is available via a unique security key allocated at the time of Your account configuration. Any unauthorised access to any BT IT systems or unauthorised modification by You of Data or computer programs will result in You being locked out of the system and a referral by Us to a prosecution agency under the relevant sections of the Computer Misuse Act 1990.

10. Provision of Information

M10.1 In the investigation and detection of fraud against the Network, You or Your agents will provide Us with such information as may be required. There may be a requirement for Us to pass this information onto a third party, e.g. the police; but this information will not be used for commercial purposes or for direct selling. You are expected to co-operate fully with BT in the investigation and detection of crime.

11. Control of Third Parties

M11.1 You will maintain and demonstrate adequate controls over any Third Party that uses or has access to

the Services that We provide to You. You must ensure that all the provisions of the UK Multi-Network IoT SIM Service Agreement and all Codes of Practice are complied with.

12. Inspections

M12.1 The BT Audit and Assurance Team may periodically require access to Your premises to make random checks on fraud prevention measures and to pursue lines of enquiries. You must support this process.

13. Advisory Fraud Protection Measures

A13.1 Outside of the provisions of this Code of Practice, there is much that You can do to protect Yourself against fraud:

a. Where relevant, make site visits to new Resellers and/or End-Users to establish bona fides of name and address given.

b. Request upfront payment for equipment and the first months' invoice.

c. Do not be predictable when requesting proofs of ID. Change the goal posts periodically and ask for varying kinds. Checks should always be made to ensure that the proofs are valid. Photographic proofs are always advisable as they are harder to fake.

d. Ensure staff integrity. New staff are a particular risk and references should always be followed up. Right to work checks should always be carried out before employing new staff.

e. Ensure delivery of any equipment is to an address linked, or known to be linked, to the End-User.

f. Be cautious of End-Users that change their requirements shortly after being accepted. For example, the initial request may be for one or two subscriptions, but when accepted, change the requirement to several more.

g. Always confirm a landline number for contact, and compare it to information available online (company website, Yell.com, 192.com etc)

14. Device Behaviour

M14.1 If a Device shows aggressive behaviour that threatens Network integrity, We reserve the right to remove it from the Network. If We notify You of aggressive Device behaviour, You must investigate and take appropriate action to remedy.

Network Operations Codes of Practice

1. Introduction

Advisory

We take Our Network and the provision of Service seriously and expect this responsibility to be shared by Us and You. This Code of Practice details the actions and responsibilities of both Us, You and any Third Party.

Two classifications of clauses are detailed and these will be preceded by **M** meaning Mandatory and **A** meaning advisory. This Code of Practice may be revised from time to time by Us and in urgent cases may be supplemented with email notifications to You for immediate action.

2. Established Processes & Communication Links

M 2.1 Before You can provide services via Our Network, the following things need to be in place:

1. Internet Connectivity

In order to Connect to BT for Data transfer purposes, You must have the use of standard internet connectivity. You may request enhanced interconnect solutions from BT (such as private APN, managed VPN) subject to contract.

2. Remote Provisioning

In order to self-provision Subscriptions and Services on the Our Network, You must either have browser access to the IoT SIM Management Platform or a customer system to utilise any available APIs. Liability and obligation rests with You for timely and accurate input for provisioning on the Our Network. Wholesale invoices will be generated from the information generated from the Data provided by You.

3. Billing

Usage activity information is available via the IoT SIM Management Platform which You may use for input into your own billing systems. We will allocate the Default Rate plan for the billing of services until You choose an alternative Rate Plan (if available).

3. Customer's Equipment Approval

M 3.1 We can provide a list of IoT/M2M Accredited Devices which is subject to change. Such Devices have undergone Network assurance testing to confirm performance of the SIM and Device against Network protocols. Although We recommend You use an IoT/M2M Accredited Device, You must still complete Your own end-to-end testing of Your IoT/M2M solution to ensure that all hardware and software functions and does not interfere with the performance of the Network. We recommend that Your end-to-end testing includes testing Your IoT/M2M solution in the actual environments You intend to deploy the IoT/M2M solution into, especially if they involve unusual operating circumstances. Examples of unusual operating circumstances would be:

- Embedding/setting SIM/Devices in resin or concrete
- Operating in close proximity with sources of microwaves
- Frequent polling, i.e. every second

We cannot guarantee access to the Network as environmental conditions can have significant impact.

4. Customer's Equipment Tracking

A4.1 You will use reasonable endeavours to develop an effective system to allow tracking of Equipment and SIM Cards that You despatch.

5. Restoration of Service

A 5.1 We will not give You preference when restoring the Service as We cannot agree to fetter how We manage the Network for the overall benefit of all Our customers.

6. Fault Service Notification

A6.1 We will in accordance with Network support processes give notice of faults or loss of Services within Our Network. This information will be notified to You by email from Us.

7. Coverage and Service difficulties

A7.1 We will endeavour to supply sufficient information to allow general coverage and service difficulties to be handled by Your support network.

8. Planned Works

A8.1 We will from time to time need to carry out planned service affecting work within the Network. Where this work is considered to be significant these will be notified to You via Network Support. This will be notified by email.

9. Mobile Telecommunication Privileged Access Scheme (MTPAS)

A9.1 Mobile Telecommunication Privileged Access Scheme (MTPAS) is provided within the UK and Europe to allow for control of traffic for emergency services and Government departments in time of emergency. In such case We can carry out controls within the Network to reduce the non-emergency traffic to allow the emergency services to operate correctly. In the United Kingdom MTPAS is authorised by the Police Gold Commander.

M9.2 We will without notification implement MTPAS which in some cases may remove Services to Resellers, End-Users and Users when requested to do so by an emergency authority or police incident officer to enable priority to be given to Emergency and Government Departments.

10. Interception of Communications

A10.1 We are required under the Regulation of Investigatory Powers Act 2000 (and other Statutory Requirement) to carry out interception of communications as defined in the above Act and for the purposes connected with the provision of postal or telecommunication services.

M10.2 You must supply name and address details in support of the Regulation of Investigatory Powers Act 2000 when requested to do so by an appropriate BT representative. We may ask for confirmation that a request has been made of You for information related to the interception of communication. This is to ensure that We can meet Our obligations for carrying out the interception and to ensure that the interception carried out by Us is in compliance with the warrant served upon Us.

11. Customer, Address and Billing Checks

M11.1 You must provide systems and processes to ensure that name and address checks can be carried out

by police and other authorities under the Data Protection Act (1998) and other Statutory Requirements.

M11.2 This information may be required by Us particularly in the cases of extortion, terrorism and in cases of threatened loss of life. You must provide on production of a DPA request from Our Network Operation Centre or Security Group immediate return of information of the Resellers, End-Users or Users address and supporting information.

12. Communications

A12.1 Good communication between Us and You is a key part of providing a quality of service for Us and Your Resellers, End-Users and Users. You should do all that is within Your power to ensure that communications between Us and You are efficient and professionally controlled.

M12.2 You must supply a dedicated email address for information from Us and maintain a telephone line for emergency or operational issues between both companies. You will provide these prior to launch of service and keep updated full contact telephone numbers, 24 hour escalation numbers and the ability to provide information when requested.

M12.3 It is important that only the contact numbers specified are used for the specified activity; misuse of contact numbers will be monitored.