TUFF Trader Code of Practice

September 2024

Table of Contents

Introduction

TUFF members first agreed a form of this Code in 2009, then called “The UK Recyclers’ Voluntary Code of Best Practice”. Since them, the Code has been instrumental in the fight against mobile phone crime and in the UK, adherence to the Code is virtually ubiquitous among commercial Buyers.

This version is a complete re-write, removing out of date language, methods and technology references and reflecting established implementations of the Code among members.

Terms Used in This Document

References to the singular also include references to the plural. For example, mobile phones typically have several identifying numbers. Reference to ‘serial number’ means all those numbers should be considered.

Member	Refers to a member of TUFF.
Buyer	Any person or business purchasing used Mobile Items, whether for re-use, breaking or repair. See Appendix B: Examples of Buyers
Code, CoP	This Code of Practice.
NMPR	The National Mobile Property Register, a police intelligence system available globally.
Due-Diligence, Status Check	The process of checking property status before purchase.
Quarantine	The separation and secure storage by a Buyer of a compromised device.
Items	Articles of property, typically consumer electronics, in particular phones, laptops, tablets, cameras, watches. They are small, valuable, often traded and carry at least one manufacturer provided serial number allowing clear identification. See Appendix A: Example Items .
Network Operator, Telco	A Mobile Network Operator (MNO) or Mobile Virtual Network Operator (MVNO)
Blocking	Refers to the denial of service from MNO/MVNOs for a device reported to them as lost or stolen, identified by an IMEI number.
Subscriber	The customer of a Telco; an individual or entity with an active service agreement to receive mobile telecommunications services.
Checking System	A computer application (whether mobile, web or desktop) that provides auditable status checks to Buyers and complies with the Compliance for Checking Systems

	section.
TUFF	The Telecommunications UK Fraud Forum, the not-for-profit author and copyright owner of the Code.
FNOL	First Notification of Loss. The date and time when an insurance claimant first contacts the insurer to notify them of a covered loss or event.

Goals

The Code seeks to reduce crimes such as theft and fraud associated with Items. It does this by:

- Defining a practical, cost-effective process for a Buyer to follow;
- Specifying what compliant members should expect from each other;
- Defining compliance requirements for different stakeholders.

Compliance achieves crime reduction by:

- reducing the ways in which a thief may convert stolen Items to cash; and
- generating intelligence to assist investigations; and
- gathering evidence to assist prosecutions; and
- removing anonymity from item movements.

Scope

This Code applies to all Mobile Items.

Being a product of TUFF, earlier versions of this Code were concerned with addressing the movement of mobile phones. Other Mobile Items are now capable of being connected to telecommunication networks and used for fraud and other crimes. These items include tablets, watches and cameras.

Buyers who buy phones as well as other items routinely perform checks on all serial numbered property. A key improvement in this version of the Code is to include such items in the scope. This may feel like ‘scope creep’ given TUFF’s name and remit, but the reality is that the Code has had such a profound impact on the movement of stolen communications devices and the investigation of the same that it feels appropriate to encompass all serial numbered property given that no comparable code already exists for such items.

Since current adherents already do this, there is no impact to their operations. We feel it is important to support and encourage this behaviour all suitable items that a given Buyer deals with, so the higher levels of due diligence extend beyond phones.

This Code does NOT apply to waste recycling activities for which established WEEE regulations apply.

Compliance for Buyers

A Buyer must:

- include in its terms and conditions, clear language explaining its obligations under this Code and the treatment of rejected items (see Appendix C: Example Terms and Conditions
-); and
- keep accurate records identifying the seller where a transaction proceeds; and
- keep IP address records and user IDs related to any online transaction; and
- obtain the item serial number as soon as possible during a transaction; and
- perform a status check for that serial number with a compliant system; and
- refuse to buy the item if the status check result indicates a compromised item; and

In the case of a compromised item the Buyer must:

- provide to the seller, an email address for the compliant system support team so they may dispute the status check results if they wish; and

If the seller is physically present,

- hand the item back to the seller. This is a requirement to protect Buyer's staff against abuse from sellers who dispute the check result.

If the seller is not present (and will not be, such as in online situations), the Buyer must:

- place the item into a quarantine area where it must stay until:
    - 28 days has elapsed; or
    - A police representative investigating a crime has collected it; or
    - The rightful owner, providing sufficient evidence of ownership, has collected it.
- advise the Seller of the quarantine status and ask which action they would like to take if after 28 days the status is not cleared, and no other party claims the item. The options being:
- have the item returned to them at the seller's cost ; or
- have the item disposed of by the Buyer, without compensation to the seller, and in a form unlikely to cause distress to any future owner (see Appendix E: Post Quarantine Disposal Examples
- Appendix D: Return of Quarantined Items

Post Purchase Actions

If the Buyer receives notification that the status of an item has changed from clear to compromised, they must:

- remove the item from stock if it has not yet been resold or reused and then follow the quarantine process.
- if it has been resold, contact the customer to advise them of the new information, and offer a refund or replacement.

Compliance for Insurers

TUFF members from the Insurance industry may also be Buyers of Mobile Items. They are encouraged to comply with the Code for such operations using the Compliance for Buyers section above.

For other insurance operations, the compliant insurer must recognise that compliant Buyers do so at some cost to themselves while creating benefits to insurers including:

- building intelligence about the movement of devices; and
- providing opportunity to recover an item for which a claim has been settled; and
- recording timing information that can help repudiate fraudulent claims.

As part of their claims handling procedures, insurers often require the claimant to have taken certain actions in respect of the item being claimed for. For example:

- making a crime report to police; or
- reporting to a police connected loss reporting system; or
- blocking phones before starting a claim.

In the case of blocking, it is not uncommon for an insurer to observe that the phone is not currently blocked and request a network block themselves. For fraudulent claims this results in damage to the good faith Buyer to whom the fraudster sold their phone before beginning the claim.

To be compliant with the Code, an insurer must:

- Provide a contact point for compliant Buyers to question item status;
- Consider the timing of a sale questioned by the Buyer; and
- If the sale took place prior to when the claimant says the item was lost or stolen (which would be prior to FNOL) then remove any restriction that is within the control of the insurer.

Compliance for Checking Systems

A compliant status checking system must:

- be certified by a UKAS accredited body to meet the latest revision of;
    - Management Systems Quality Standard ISO9001; and
    - Information Systems Management System Standard ISO27001.

It must:

- provide a clear warning to the Buyer when a Mobile Item is compromised, meaning its legal title is in doubt; and
- record all status checks and results on national police systems to ensure prompt visibility to policing; and
- generate alerts to registered owners when a Mobile Item has its status checked; and
- provide robust support and dispute resolution processes for Sellers; and
- be capable of providing supporting documentation to evidential standards including witness statements and ability for the operating company to undergo cross-examination in court if required to do so.

It must consult data about mobile items from many sources, including:

- mobile network operator blocking records (only relevant to phones);
- loss and theft reports made to police;
- loss and theft reports made by the public;
- settled insurance claims;
- known counterfeits or clones;
- corporate and privately owned items prohibited from resale.

It must be capable of:

- alerting the Buyer when a previously clear status check, if repeated now, would show as compromised; and
- it should provide this alert for changes up to 30 days after the original clear check; and
- it must alert originators of negative records (where they have elected such) to the buying activity.

Appendix A: Example Items

Examples (not exhaustive) other than mobile phones where you may see a manufacturer provided unique serial number are:

- games consoles
- cameras
- watches
- laptops
- personal computers
- bikes
- graphics cards
- CPUs
- printers
- monitors and TVs
- power tools
- batteries.

Appendix B: Examples of Buyers

This list is not exhaustive and serves only to provide examples of trading situations to which this Code may be applied.

- An Insurer is buying used Mobile Items from companies to provide replacements to claimants. The Insurer is the Buyer. We recommend the Insurer complies with the Code and makes it a condition of sale that the seller does too.
- A recycler offering to buy used items online which are then sent to a warehouse before any serial number is available. The recycler is the Buyer and should comply with the Code on receipt of the item.
- A manufacturer accepting phones from consumers as a trade-in against a new device is a Buyer and we recommend compliance with the Code. If using an intermediary to deliver the trade-in service, we suggest the intermediary is required to comply with the Code and any tender for new partners makes this a requirement.
- A bricks and mortar retailer of used items should use the Code to avoid buying stolen property. This is a favoured disposal route for criminals and failing to perform due diligence will lead to the retailer and their onward customer potentially becoming victims of a dishonest seller.
- A repair workshop should consider themselves a Buyer and act accordingly. While they may not be buying the items, if they intend to keep them and provide a replacement then they are at risk of being used to launder stolen devices unless they also comply with the Code. The replacement items of course should be checked when they are first acquired, also and ideally, before providing as replacement though this secondary check does not form part of the Code.

Appendix C: Example Terms and Conditions

Your terms and conditions will be reviewed during the compliance checking process and must be clear and obvious to your customers. The following is offered as an example that would meet TUFF's compliance requirements. You should seek legal advice specific to your business before using any wording.

> "We comply with the TUFF Code of Practice (link to code on TUFF website). All items offered to us will be checked for lost, stolen and other records that would make it impossible for us to buy the item. For items sent to us rather than checked in person, we will withhold payment and quarantine the item.
>
> Quarantine provides up to 28 days for you to clear the status of the item. It is possible that the police, an insurer or anyone else who can evidence ownership of the item that pre-dates when it was sent to us, will retrieve the item during the quarantine period. If this should happen, you will not be paid for the item. Please do not send items that you know, or suspect may be stolen, or that you found, are renting, or have loans secured against.
>
> At the end of the quarantine period, if the status is not cleared and the item is unclaimed by a rightful owner, you will have the choice to pay for return shipping costs or ask us to dispose of the item securely. You will not be paid for the item. "

Appendix D: Return of Quarantined Items

Buyers should keep in mind that the rightful owner of any item always remains so. The effort you have expended complying with this Code and the investment you made in marketing to bring sellers to you, in no way changes the owner's rights under the law.

In many jurisdictions, ownership rights may only be transferred by the current owner. Therefore, a compromised device that ends up in your possession without the agreement of the owner must always be returned to that owner if it is possible to do so.

We encourage owners, and corporate owners in particular, to recognise the value in Buyers' efforts to comply with the Code and trade responsibly. We recommend that when recovering their property from a Buyer's quarantine, owners consider making some contribution to the Buyer's losses.

Existing practice in this area has led to formal agreements between insurers and Buyers that the insurer will accept a discounted used value for the device or pay a modest recovery fee to reclaim it.

Owners should remember the Buyer came into possession despite taking all precautions to avoid compromised items. The Buyer has no obligation[1] to return the item at their cost. The owner should expect to pay for shipping. If the owner doesn't wish to do so, they always have the right[1] to attend the Buyer's premises and collect their property.

Of course, anyone claiming ownership must be able to show the Buyer evidence of that ownership such as an original receipt. It is beyond the scope of this voluntary agreement to design a mediation process between a claimed owner and the Buyer. If the owner believes the Buyer is behaving unreasonably, they have the recourse of reporting to the police to determine if the Buyer might be guilty of theft by continuing to hold the item.

It is worth remembering that since 2009 there have been over 600 million global transactions compliant with this Code and we know of just a few cases where a serious dispute has not been quickly resolved.

Most owners and Buyers are reasonable and know they are in this together. Mutual respect and cooperation work.

[1] In the UK anyway; always check legislation in your region.

Appendix E: Post Quarantine Disposal Examples

These are examples of how the compliance requirement for disposal after quarantine may be met for different types of item compromise. As this is dealing with the disposal requirement, it should be assumed that the 28-day quarantine period has elapsed, the record originator has not collected, and the seller has indicated the Buyer may dispose of the item, or they have not responded in a reasonable timeframe. These are not prescriptive; they just serve to illustrate what considerations may be relevant to the Buyer.

To satisfy the requirement of not causing distress to a future owner, the nature of the compromise needs to be considered.

Scenario 1:

The reason for compromise is a settled insurance claim. The insurer has been contacted but neglected to arrange repatriation. The Buyer may request the compliant system operator to remove the negative record. If the insurer agrees, then the record will be removed, and the Buyer will be able to sell the item without future ill-effect.

Scenario 2:

The reason for compromise is a network block. The Buyer may request the compliant system operator to remove the negative record, but this is unlikely to succeed in our experience. The Buyer may be tempted to sell the item internationally, knowing that the national blocking may not be in effect and so the item may work. However, this fails to be compliant as it has the potential to harm the end customer should they travel to the block-originating country. In addition, since compliant checking systems should operate globally, such a device would still be rejected everywhere. In this situation breaking the device for parts may be the best option for the Buyer to recover some cost, space and return for their efforts, having exhausted all legal routes of repatriation. Of course, any such action should be compliant with the law. Being written here does not make it lawful, this is a guide.

Scenario 3:

The reason for compromise is a police record. The compliant system operator will seek confirmation from the originating force that the record is an error of some kind since they have shown no interest in retrieving the item for evidence or to restore to the victim. Failure to confirm this will result in the compliant system operator removing the record (from its own records, not the original police record). In the absence of any other indicators of compromise, this would then render the device tradeable.