THE SPECULATIVE INVOICING HANDBOOK

Second Edition

Disclaimer

This document is for informational purposes only and does not provide any legal advice; it should not be interpreted as doing so. Neither the contributors, authors, publishers or distributors accept any responsibility or legal liability resulting from the use or misuse of the information presented in this document or any of the resources referred to within it.

You accept in reading this document that you do so at your own risk.

Any views and opinions expressed in this document do not necessarily represent those of the author.

Dedication

In memory of Oliver.

Cover picture credit: reway2007 (http://www.flickr.com/people/reway2007)

Stage One: Put The Kettle On

So you've received a letter, you feel intruded upon and threatened. You're wondering if you even did what you've been accused of – well, at least, what your *connection*, has been accused of…

You're far from the first and you're *unlikely* to be the last to get one of these 'nastygrams'.

The first step to managing the situation you've been put in is to tackle it calmly. You have been invited to play a game. This particular game requires careful thought and rational, planned actions. It is not best played while emotions are running high; never do anything in haste.

You're reading this handbook so you've clearly used your head so far and are on the right track.

If you've not already done so, make yourself a cuppa and sit down to read the rest of this. Relax… you're among friends now. Welcome to the team.

Photo credit: Mark Thurman
(http://www.flickr.com/people/mthurman)

Stage Two: Don't Make a Bad Situation Worse *or* Quick Advice to Get You Started

- Don't write *anything* about this for at least 48 hours… blog posts, letters, emails, forums… *nothing.* You'll figure out why later.
- Don't get drunk (yet).
- Wise man say: be selective where you go for information. In other words – there's a lot of bad advice out there. Think carefully before acting on any of it.
- Understand the ins and outs of your own situation. Only you know your own particular circumstances. No one can tell you exactly what to do. You need to review the information and make your *own* decisions.
- Play as part of a team. It's the only way you'll win this.

What *is* Speculative Invoicing?

In short, speculative invoicing (also known as 'volume litigation' and 'pay-up-or-else') involves a firm sending large volumes of letters. Each letter contains a demand for cash, accompanied by an allegation that the letter-writer's copyright has been infringed. The monetary demand is usually presented as a settlement which is, they say, at an appropriate level to make good the potential losses incurred by the copyright owner. The letter will threaten the recipient with court action and potentially massive costs should they not accede to the request to settle swiftly at the level stated.

There are a few universal features to these letters:

- they are almost always sent to a person that has not infringed the copyright
- the settlement figure proposed is almost always ludicrous (typically ten times higher than might be expected had an infringement of copyright actually taken place)
- there will be a COMPLETE lack of any evidence to support an accusation of copyright infringement against the letter recipient
- they feature a heavy preponderance of 'doublespeak' (for example, letters will appear to state a strong likelihood of impending court action and high costs should the recipient not settle, but in fact such claims are carefully stated using terms which disguise the remote possibility of such an event taking place; viz, '*in the event* that it becomes necessary' 'it *may* become necessary' 'consequences against you *could* follow')

The letters rely partially on a recipient's naivety of law, but mostly on fear. They are wholly unpleasant as, one could logically conclude, must be the people who choose to send them.

A Quick Introduction to Peer-to-Peer File Sharing

Peer-to-peer (sometimes referred to as P2P) file sharing is a means by which data can be shared between computers. Traditionally on the internet a home computer would have connected to a web server (typically a much more powerful computer, owned by a company or an organisation rather than an individual) to download large files that users wanted to access. These files might have been software, music or other entertainment media, documentation or any other type of file.

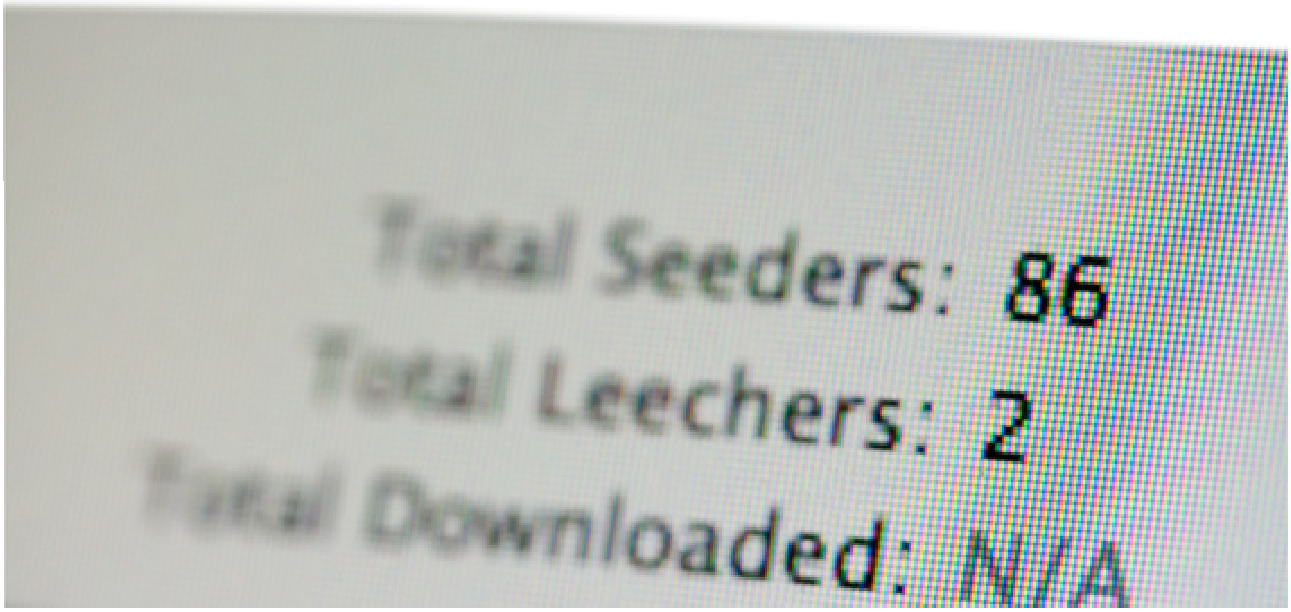
This model for the distribution of files evolved over time. Running servers is costly, and ensuring that the files required are available on servers depends on someone with a server making them available – something that might not be possible, for instance, for an independent musician or a lone software developer.

Peer-to-peer technology developed. When files are shared peer-to-peer there is no 'major' server. Instead, a number of the home computers connect to each other. Generally a number of these computers will hold a copy of the file desired by another user. Each of them will share a portion of the file with the person wanting it. The process is automated and the technology pretty much looks after itself as far as a download is concerned.

It may take some time to download a file. At the same time as the computer is downloading one section of the file it is quite capable of *uploading* a part it has already received to someone else who also wants it. Indeed this is the fundamental principal of file sharing. If no one uploaded, no one would be able to download.

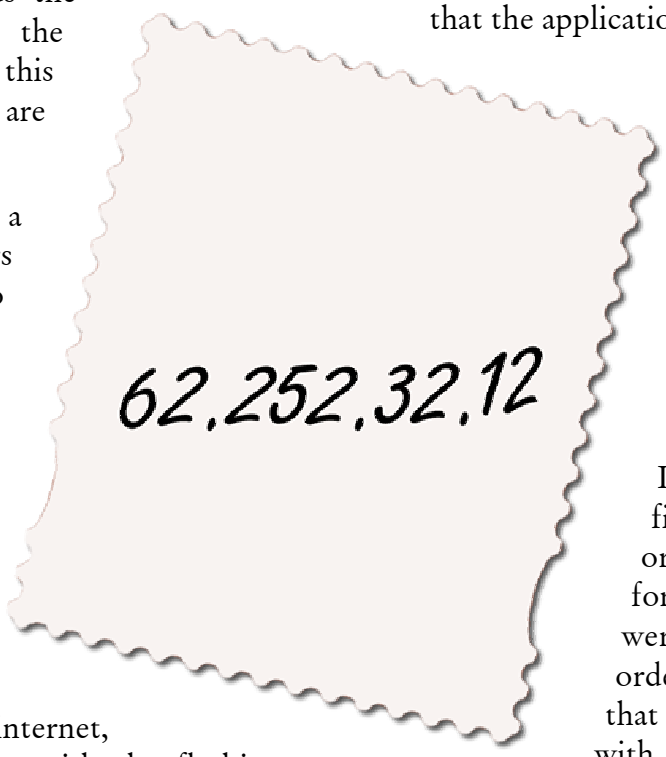
Peer-to-peer is most often publicised in a negative context – that of unlawful file sharing – infringing the copyright of others. It is worth noting however that file sharing itself is not unlawful, and there are many legitimate uses of the technology.

Photo credit: NRKbeta (http://www.flickr.com/people/nrkbeta)



What You Could Fit on a Postage Stamp *or* Examining Their Evidence

The 'forensic computer analyst' (or whatever they're calling him this week) providing the data which have led to you receiving a letter uses a program which sits on top of a piece of peer-to-peer software. That connects to a collection of computers sharing a file via peer-to-peer technology (a 'swarm') and records the IP addresses of the connections which this software indicates are sharing the file.



An IP address is a bunch of numbers strung together to create a kind of temporary 'reference point' so that computers and other technological hardware can talk to each other efficiently. When you connect to the internet, your router (the box with the flashing lights that plugs into your wall port) gets given an IP address by your Internet Service Provider (ISP). It might look something like this: 62.252.32.12

Most people do not have a 'static' (unchanging) IP address. Your router will usually be given an IP address for a period of time by your ISP. This will change from time to time; this arrangement is called a 'dynamic' IP address.

First important point: in 99.9% of cases it is *extraordinarily* likely that this is the whole of their evidence: a piece of mystery software providing a set of numbers…

The problem for them now is that having gained a record of an IP address… how should they exploit it… or rather more… with *whom* should they exploit it…

The firm applies to a court for a Norwich Pharmacal order 'against' your ISP (usually after conferring with your ISP to ensure that they will not contest the application for the order; if they did, the chances are that the application would be dropped).

Once granted, the order 'forces' your ISP to match the IP addresses gathered by the speculative invoicers' software with the personal details of their account holders. Not that there was anything forcing the ISP to pre-agree with the firm not to contest the order, but it sounds better for an ISP to say that they were compelled by a court order rather than to admit that they wholly cooperated with the people sending their customers threatening letters.

Typically the order gets granted.

In theory the combination of time slot and IP address will enable the ISP to match every recorded infringement with one of their subscribers. In fact this doesn't work. In the past an IP addresses was actually matched by an ISP to an individual who, although a customer, had *never had an internet connection through that company*. And typically about a *quarter* of all IP addresses cannot be matched to any account. That's how reliable IP address evidence is, and this firm is relying on it to send you threatening letters. That should say something about their standards.

The Five-Point Plan to Stop Speculative Invoicing

Do NOT Give Them Your Money

The letter you have received is part of a scheme designed to extract as much money as possible, from as many people as possible, as easily as possible. Do not be under the illusion that the primary intention of the scheme is to deter internet piracy. In fact, a presentation by one of the companies that operates this scheme makes clear that piracy is very profitable. Claims of the type you have received can bring in 150 times the money that would have been made had a legitimately purchased copy of the work been sold.

The only reason this scheme continues to operate is that someone believes it to be profitable. Where does this profit come from? People like you – scared into paying up *by a letter designed to do just that*.

At the time the first edition of this handbook was written, it was claimed by one of the companies carrying out this work that 15-40% of people pay up (depending on the title in question) – no questions asked.

Without an income how much longer would the scheme last? Perhaps until they'd run out of stamps. Not much longer. People like you are their *only* source of money. It is important that you part with as little money as you possibly can. I can tell you now the exact percentage of the 60-85% of people that didn't pay that ended up in court. ZERO. The scheme relies on easy payers.

If you send them £700 (a typical sum demanded) consider how that will support their business. How many more letters can they afford to send with *your money*? One of them might be another letter to you…

As I sit here, three years after that 15-40% claim was made, I'm now in a position to tell you how effective it is when people refuse to pay. Thanks to a concerted community effort, the revenue stream of the firm that made that statement dried up. Bankruptcy followed in less than a year.

The very fastest way we can stop this is to cut off their money. Not only is this quick and easy, it also means you save £700.

What you do: **Not pay.**

Destroy the Business Model

Further on in this handbook you will find a section that diagrammatically sets out how exactly the speculative invoicing scheme works. There are clear weaknesses in the plan; it is these that have to be exploited to stop these businesses in their tracks. Let's look at a couple of those:

1) The 'pre-compliance' of your ISP

At present the speculative invoicers confer with ISPs in advance of the application for the Norwich Pharmacal order. Ordinarily the firms will only apply for an order to be made against an ISP that has previously agreed that they will not contest the application (ie. the ISP will not question the validity of the information supplied as evidence against you). Unless they have changed their minds since the order releasing your details was signed, your ISP was one of them. Your ISP did not consider that it was worth their time or effort to protect you from the threats that they knew would follow, despite being fully aware of weaknesses of the information cited as evidence. The ISPA – the ISPs' own trade association has stated that they are "*not confident*" in the abilities of the data collectors to correctly identify copyright infringing users.

Three facts:

- An ISP is a business.
- If they don't protect you it's because they don't think it's worth it.
- As their customer you have the perfect chance to show them they're wrong. Cost them money – ditch them – and tell them why.

The Norwich Pharmacal orders are typically for thousands of disclosures at a time. Potentially thousands of lost customers. That's not something that ISPs can afford to ignore. And because this is now the second edition of this handbook it can include an example that'll show you this works:

In November 2009, ISP BT allowed an order to be made against them, uncontested. It related to 25,000 IP addresses. It was estimated that these would translate to approximately 15,000 BT broadband subscribers.

The customers that got letters as a result of BT failing to contest *that* court order nagged, pestered, complained and shouted from the rooftops how completely *furious* they were with their ISP. The result: in September 2010 when another company tried to obtain BT's customers' details, the ISP was a little wiser. BT stated their intention to contest the order in court and the application was dropped like a hot potato. The letters never went out and many thousands of their customers were spared the aggravation and stress of a series of threatening letters. Success.

Sadly, not every ISP has yet had that awakening. Make it very clear to the ISP that stitched you up why they're losing you. Eventually all ISPs will learn; sometimes it has to be the hard way.

What you do: Ditch your untrustworthy ISP. Start your notice period NOW. Oh, and tell them why.

2) Income

People like you are the only people funding this unpleasant scheme. Their dependence on your money is their biggest weak point. Exploit it. Be happy (okay, you might not feel like being happy right at the moment, but bear with me…) – you have the means to kill off a really slimy business. You have the means to make the world just a little bit better. And it's as simple as not giving someone your money (now that's a rare opportunity).

What you do: Not pay (did we say that already?)

Read Their Rules and Refuse to Play by Them

In November 2009 documents used by some the companies that were then involved in the speculative invoicing scheme were leaked onto the internet.

Those particular documents showed that the firms assigned a 'litigation rating' to their victims. Essentially it highlighted how worthwhile it was likely to be for them to pursue an individual. It was based on a large number of factors, few of which were in any way related to the strength of their supposed 'evidence'. Primarily it was based on a victim's technical and legal knowledge, the potential that litigation might produce poor publicity (such as when a couple of pensioners were misidentified as file sharers of pornography - oops) and the likely state of an individual's finances (ie. if you have money that they believe they can extract from you).

Not much has changed in that regard…

Your ISP didn't tell the company how old you are. They didn't say what your income is, if you have children, how many people live at your house, how your computer is configured, the length of your password, if you have a solicitor. Anything they know about you is either something they've found on the internet, or something you tell them.

In simple terms: *their system works because you tell them stuff.*

If you are innocent and stick to a straight denial you will be one of thousands of faceless unworkable claims. The minute you tell them about you they start ticking boxes, using the information to potentially find out more about you and most importantly – you become a real person to target – something beyond the IP address they started with.

Turn out the lights. Leave them in the dark. Tell them nothing.

The only time you should provide any information is if and when they supply any evidence to support an accusation against you personally. This has never happened to date. In the event it does, see a solicitor.

In the past at least one firm has sent out questionnaires to victims, which they were told they MUST complete (and it was written like that, in block capitals). You are under no such obligation. Pre-action procedure does not require the answering of questionnaires.

If you 'reply and deny' and subsequently receive a letter from the firm requesting further information: Congratulations! That should demonstrate to you that they don't have enough information to build a case against you.

They're hoping you'll be kind enough to fabricate a case against yourself (or maybe someone else) on their behalf. Perhaps you'll be good enough to suggest your own grandmother who surfs eBay for knitting supplies when she pops over on Sundays? Maybe your younger brother or your flatmate? Thankfully you're not as stupid as they'd believe. You tell then *nothing*.

There are More of Us. Exploit This.

You are just one of many thousands of victims. The most effective way to have an impact is as part of a team. Keep yourself aware of developments and help the group effort where you can.

In the history of the scheme there have been many victims that have been content to sit back and let others do a lot of work on their behalf. That doesn't help. The websites you have used for information didn't happen overnight – they took work. You might have heard about the sites from a story on a news site – that'll have been the result of a press release someone wrote. All of the research, publication of leaked documents, template letters of denial, background legal information, website design and creation of resources have taken people a very considerable amount of time to produce.

Many hands make light work. While there are loads of us, please make sure you play you part. As I'm typing this handbook it's a quarter to midnight. It's work, but it's worthwhile. Please do *your* bit too.

Understand That in This Story the Good Guys Win

Three years ago, when the first edition of this handbook was written, it was solicitors that ordinarily used to operate the speculative invoicing scheme. They would find content creators willing to sign over their copyrights in return for a share of the proceeds of the scheme. The solicitors would run the scheme and rake in the bulk of the cash.

Solicitors won't operate this scheme in the UK any more. Why? Well, a couple of things happened. Firstly, the victims got really *really* annoyed. Secondly, they and their supporters combined their forces as a massive and incredibly powerful team. The concerted effort of those people had an awesome and devastating result on the speculative invoicing solicitors.

Those affected wrote to television companies; they emailed radio stations and newspapers; they wrote to their MPs and members of the House of Lords. They shared their stories online. They created websites and blogs and uploaded stuff to YouTube. When the firms went to the ISPs for the details of more victims they sat in the back of courtrooms and tweeted activity minute-by-minute or scribbled furiously into notepads. They nagged, incessantly, their ISPs to act. They attended meetings in parliament, responded to consultations, worked with consumer bodies to educate the public and did all sorts of other wonderful crazy things.

Very successfully, they also complained in massive numbers (as in, over 500 complaints about one solicitor alone) to the Solicitors Regulation Authority (SRA).

There's a vaguely amusing little anecdote there; excuse me while I meander off course for a moment. At around the time that these complaints were made there were live televised debates going on in the House of Lords which, in part, were concerned with speculative invoicing (because a number of Lords had been lobbied by victims).

During one debate it was stated by one Lord that the SRA hadn't received any complaints about the law firms participating in speculative invoicing (which was wrong, to say the least). A sizeable number of the 500 complainants became aware of this statement and bustled off to contact the Lord in question. A day or two later on television we hear the same Lord speak again, *"having put various statements on the record on that day, I was inundated with correspondence. The impression was that the Solicitors Regulation Authority had received no complaints about the activities of [these speculative invoicing law firms]. In fact, there has been a torrent of complaints to the SRA."* Quite right, there had. There was a chuckle from those sat at home. Interactive TV!

But back to the matter at hand…

The result of this concerted team effort:

- there is now a thriving online support community and a wealth of information available
- speculative invoicing has been repeatedly and harshly condemned in the House of Lords
- it was openly and repeatedly condemned by consumer group Which?
- the practice was exposed in features on the BBC's Watchdog and The One Show
- it was exposed in the tabloid and broadsheet press
- the Solicitors Regulation Authority acted against three firms of solicitors (the fourth firm - the only other UK firm that touched this - never really got started, forced out of the game when they came up against a challenge from BT a few months into their activity [and that challenge from BT was spurred by complaints from past victims!])
- two solicitors from one law firm and the sole principal of another were suspended from practicing by the Law Society
- every firm was ordered to pay massive amounts of money to the SRA
- every law firm was forced to abandon speculative invoicing; the newly coordinated and informed victims simply wouldn't pay
- the (ex-)solicitor that generated over 500 complaints to his professional regulator was subsequently forced into bankruptcy by HM Revenue and Customs as the result of his speculative invoicing outfit imploding spectacularly in court when challenged by some gutsy and determined letter recipients

So, bullying solicitors eliminated… NEXT!

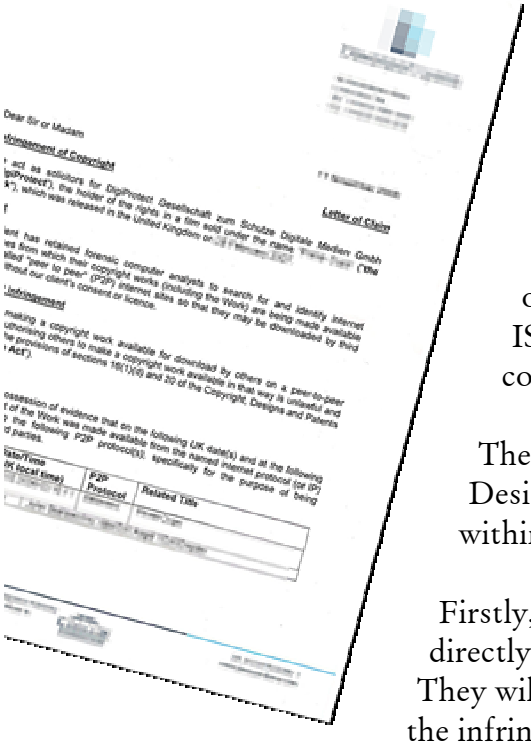
Photo credit: Images of Money (http://www.flickr.com/people/59937401@N07 / http://www.taxbrackets.org)

Top Five Frequently Asked Questions *or* Things We Ought To Make Clear

Is this a scam?

Technically this is not a scam. While the way the scheme works has much in common with a scam, the letter is genuine and is intended to be a legally valid 'Letter before Claim'. The letter you have received should not be ignored. However, this is not to say that the letter is necessarily correct, morally sound or legally indisputable.

What if I didn't do it?


Dear Sir or Madam

Letter of Claim

Infringement

Related Title

There's an excellent chance that you didn't do it. The claim you have received is based on data concerning an IP address. This is connected to a piece of hardware, not an individual human being. As such it is impossible for anyone outside of a household (and possibly even those within the household) to know who committed the infringement - assuming such an infringement even occurred. Remember it has not even been possible for the ISPs to link all of the IP addresses collected by these companies to valid accounts.

Their accusation relies for its legal basis on the Copyright, Designs and Patents Act 1988. There are a number of factors within this act unaddressed by the letter you will have received.

Firstly, section 16(2) of the act requires a person to either directly infringe copyright, or authorise someone else to do so. They will be utterly unable to state who carried out or authorised the infringement. That, alone, is a titanic hole in their case (or, an iceberg-sized hole in their titanic of a case, if you prefer).

It is also vital for a valid claim for it to be demonstrated that the sharing was of the whole or any substantial part of it (Part 16(3)(a) of the CDPA 1988). You will note that no evidence of this is presented. It is wholly unlikely in the case of large files, that even if a work had been shared, a substantial part of it would have been made available from one peer, the idea behind bittorrent file sharing being that usually a number of peers will each share a small portion of the file. It would seem highly unlikely, given the massive numbers of infringements allegedly recorded that a full instance of the file would be downloaded and recorded as evidence to support each claim.

Challenging a claimant to produce evidence that would support an assertion that a 'whole or substantial part' of it was shared from your connection generally provides a tellingly vague and wriggly response.

The letter before claim depends heavily upon doublespeak, missing information and the intention to provoke fear. A large part of it is hokum – particularly where claims are made that a court case is likely if you do not settle. This is demonstrably untrue.

Should I reply to the letter?

The decision is ultimately yours but generally, yes, you should provide at least a short reply. In legal undertakings there is something called pre-action procedure and sending a reply is part of that.

There are three related things you ought to know about. This is the most boring part of the handbook. Bear with me and we'll try and get it over with quickly:

1) **The Practice Direction for Pre-Action Conduct**

A document called the Practice Direction for Pre-Action Conduct sets out a series of stages which ought to be followed in this sort of situation. The intention is that, as often as possible, cases will resolve themselves before any court action might become necessary.

That document states that you ought to reply and specifies the nature of what you ought to say in your reply.

The relevant document can be found online for download (at the time of writing, here: http://www.justice.gov.uk/courts/procedure-rules/civil/protocol). The three pages of 'Annex A' are the relevant bit. They are three pages you ought to read. They also happen to be in the appendix of this handbook.

2) **Pre-Action Protocols – just for information, this one**

Some type of civil claim (for example, defamation and professional negligence) have their own specific pre-action protocol. Happily *there is no such protocol for intellectual property claims*. There was an attempt to draft one some years back, and indeed the draft code was published (the 'Code Of Practice For Pre-Action Conduct In Intellectual Property Disputes') – but that document was never adopted by the courts.

I'm only mentioning it because in the past at least two outfits have made mention in their letters before claim to the Code Of Practice For Pre-Action Conduct In Intellectual Property Disputes, which they oughtn't've. In any case, it actually says much the same sort of thing as the document I just described in (1).

3) **Part 63 of the Civil Procedure Rules – you barely need to know about this at all**

In the unlikely event that things ever move beyond 'pre-action' and a claim goes to court then Part 63 of the Civil Procedure Rules also becomes relevant, but given the remote likelihood of that ever happening, and the fact that those rules are almost wholly a set of obligations on the claimant, I wouldn't suggest that you worry about that *at all*. I'm just telling you about them for informational reasons, and so that you can impress your friends with your in-depth knowledge of Intellectual Property law.

It is a good idea to comply with the pre-action procedure as far as possible. In the extraordinarily unlikely event that a case ever went to court a judge would be expected to look favourably upon efforts to engage correctly in pre-action (and inversely it might be frowned upon if letters had simply been ignored).

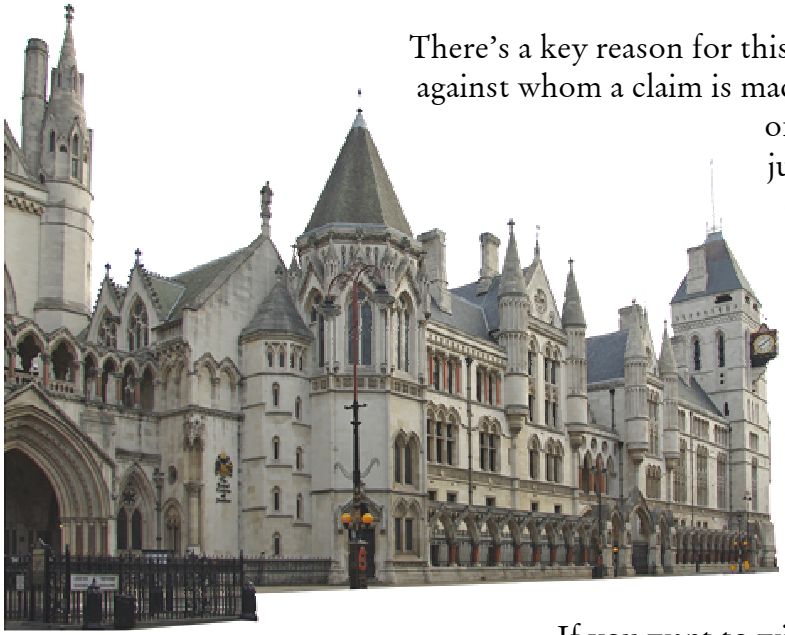
Do I need a solicitor?

Making use of a solicitor, or paying a visit to your local Citizens' Advice Bureau, is very unlikely to damage your case, however unless they are specialists in IP law, or have experience in dealing with these cases they may not be of much help. The retention of a solicitor is an expense that will need to be considered in light of your own circumstances. A lazy solicitor may be inclined to simply tell you to settle, even if innocent. This would seem rather absurd.

A very considerable proportion of letter recipients (the vast majority in fact) deal with the correspondence themselves and there is no indication to date that they have been unwillingly separated from any money or suffered anything worse than those that have appointed solicitors. Generally you can just expect to receive a handful of poorly written, threatening letters.

Has anyone been taken to court? / Will I be taken to court?

Has anyone been taken to court? Yes. Well, at least, some claims have been filed with courts. Now quickly read the rest of this before your heart rate gets out of control: generally these have been against people that have *failed entirely to reply to the letters before claim*.



There's a key reason for this. If a respondent (that's a person against whom a claim is made) doesn't show up in court, it's often possible to get a 'default judgment' – in other words, the claimant wins the case without a proper contested hearing. A default judgment, when spun appropriately in a press release, is a useful scare tactic to use against other letter recipients. Someone lost a case in court! This evidence must be devastating! I must settle immediately! Where do I sign?

If you want to win default judgments it makes sense to choose people that are very unlikely to turn up in court. Therefore you don't choose people that answer the letters. The default judgments are not primarily about winning damages; the main value is in the fear they can create – in those that don't understand how the system works. Now that you've had it explained, that shouldn't be you.

Even attempts at default judgments are *extraordinarily* rare, and have rarely been successful.

In the history of speculative invoicing in the UK (bearing in mind that, at the time of writing, around fifty-thousand letters before claim have been sent) somewhere between about five and

ten cases (it's hard to be exact, even the current judiciary can't pin down exactly how one or two cases ended) finished up with either an upheld default judgment, or an out-of-court settlement once the claim was started in court. That equates to two *hundredths* of a single percent of letters of claim ending up in court and not resulting in the speculative invoicers getting torn apart by an angry judge (which is the more usual outcome – a couple of firms imploded spectacularly in this very circumstance).

Now ask me a different question. What's that you say, 'how many times has a claim that went to court continued once a letter recipient stated an intention to challenge the evidence?'

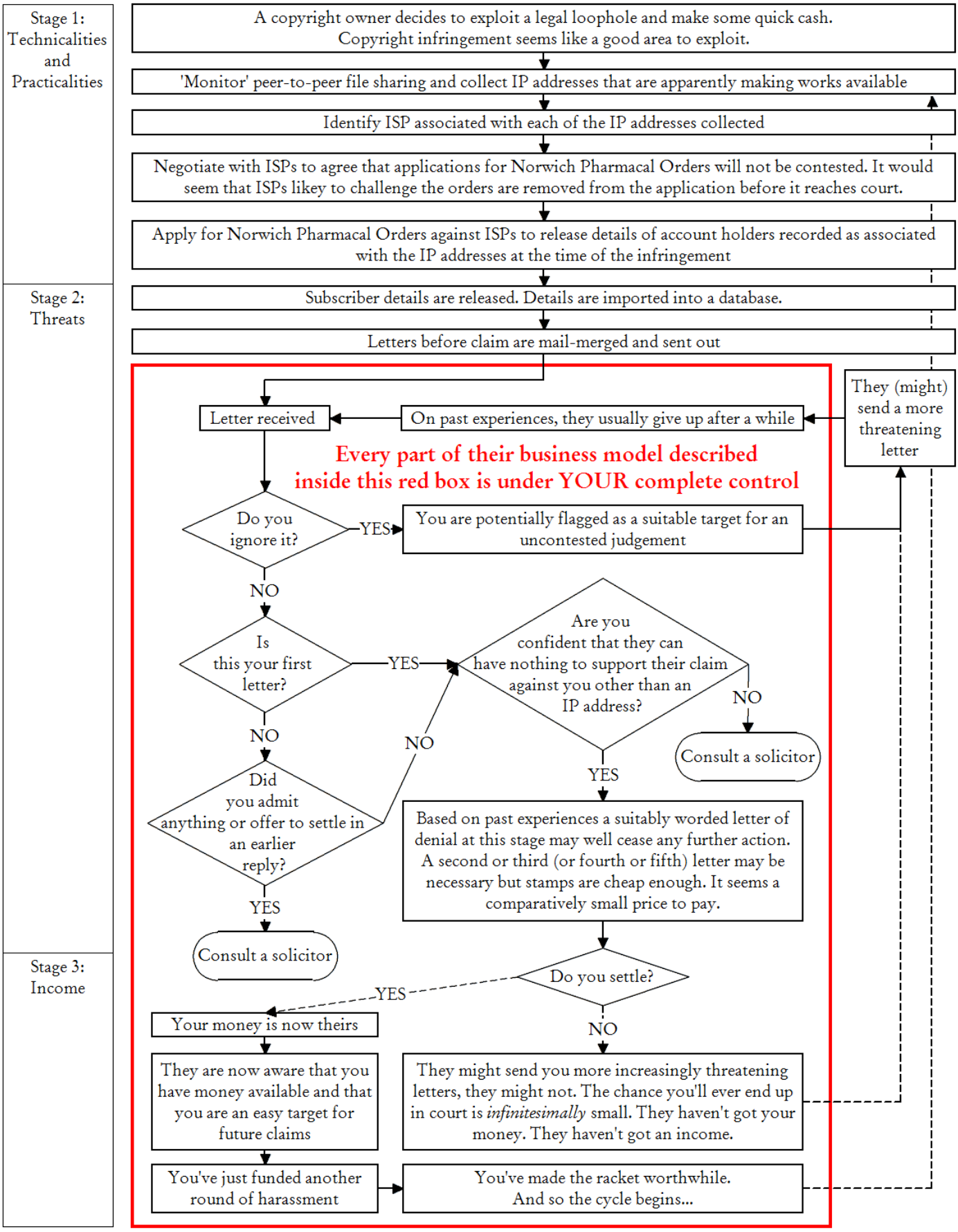
Ah! Good question! NONE. Never. Hasn't happened.

The 'evidence' which the speculative invoicers have, which we looked at briefly earlier, is flimsier than a wet paper bag; it holds about as much water as an inverted teaspoon. To date NONE of the speculative invoicing firms has dared to expose the inadequacies of the evidence in court. NEVER has their infallible 'forensic evidence' seen the light of day.

Will you be taken to court? You may draw your own conclusions, but it may be helpful to consider the facts of your own position (some of which you may not be aware). Within this handbook you will find information which will help you evaluate your own case.

Picture credit: Steve Thoroughgood (http://www.flickr.com/people/andytakersdad)

Understand How It Operates - The Key To Beating The Scheme



Five Big Misconceptions

This is a scam / This is illegal / This firm in some way aren't right

There are a whole heap of reasons why you might be inclined to reach this conclusion. The operations are certainly far from what many might consider to be professional.

You might have found other 'information' which supports the idea that one of the companies is not quite what it seems. Stuff like:

- "Their address comes up as another company!"
- "Companies House says they're dissolved!"
- "Their website looks as thought it was designed up a five year old!"
- "This letter isn't from a law firm."

While some of these observations may be correct, some may be partially correct - and others plain wrong, the fact remains that the letter you have received needs to be dealt with correctly. It is intended to be legally valid.

Ignoring the letter is the best way to deal with it

In a previous chapter you'll have found a section providing an answer to the question 'Should I reply to the letter?' While the decision is entirely yours, generally advice is that a response should be provided. The letter should not be ignored.

I checked and the IP address in the letter isn't mine

Most people do not have a 'static' (unchanging) IP address. Your router (the box with the flashing lights that connects you to the internet) will usually be given an IP address for a period of time by your ISP. This will change from time to time; this arrangement is called a 'dynamic' IP address.

There was more information on the details of the data the companies present as evidence in the earlier chapter: *What You Could Fit on a Postage Stamp* or *Examining Their Evidence*

If I pay up they will stop bothering me

Paying makes it clear to them that you have the financial resources to meet their demands. It also indicates that you are unwilling to fight them. It may also be interpreted as an admittance of guilt. If you sign an 'undertaking' admitting guilt, this is quite certain.

Many people have received more than one letter of claim; these may arrive at any time and may concern an entirely separate claim. They may rightly expect that if you have settled for one work you will very likely be worth pursuing in future – potentially in court.

Besides, why would you pay for something you did not do?

Innocent until proven guilty

This is one of the most unexpected and unsettling pieces of information for newcomers to this situation who have not previously been involved in civil litigation:

'Innocent until proven guilty' is the standard of proof required in *criminal* cases (ie. brought by the government). You are being threatened with a *civil* claim. Civil cases are assessed on the 'balance of probabilities'.

Do not be unduly alarmed however. The burden of proof remains with the claimant. They must demonstrate that you either did, or authorised someone else to copy or share the whole or a substantial part of the copyright work. There has never been a case in the UK where someone has been found guilty of this type of infringement using solely IP address evidence. There is also no trustworthy information to suggest that the companies involved have any intention of letting a case ever see the inside of a courtroom.

The standard of information presented as evidence in the letter you have received is really lousy.

Assess Your Position
or Time You Knew What They (Think They) Know

If you've received a letter there are three main possibilities:

1) You did it
2) Someone else did it
3) No-one did it

Regardless of whether you did the deed or not, you need to know what the speculative invoicers know in order to be able to respond in a sensible manner.

They start off with extremely limited information. The first step in their process as you will know by now, is to apply to the courts to obtain your name and address (and potentially your telephone number and email address) so that they can write to you.

With any luck you'll pay up, no questions asked. If not, there's a good chance they'll invest a little time in some research. They will see if there is anything they can find to strengthen their case (because what they've got so far is next to useless).

Here's what they start with:

- An IP address
- Your name
- Your address (including postcode)
- The name of your ISP
- The name of the work shared
- The nature of the work and related works (ie. other tracks by the same artist in the case of music)

Potentially also…

- Your telephone number
- Your email address
- Knowledge of the type of router your ISP will have supplied
- A username (if the file was shared, and via eMule or eDonkey or similar software)
- A username (if you choose to post about your letter on a website using your usual username)
- Knowledge of which site made the tracker available – and the ability to collect the usernames associated with that site
- If you have participated in file sharing, knowledge of other works you may have shared or downloaded

They will use this information to scour the internet and see if they can find anything which looks incriminating. It does not matter to them whether or not anything they might potentially

find is actually evidence against you or not, so long as it *looks like is*, so they can bully you with it.

You need to make sure that you are aware of what they might try to use against you. There's a reason for this. Their evidence has never (as in never-ever-ever) yet been challenged in court – because the firms have always backed out before they got that far. However, some 'court claims' have been issued. While these are simply one step on from a letter before claim, they do require more effort in terms of response and usually the appointment of legal representation as a defence against the claim will have to be provided. These court claims have tended to be issued against individuals against whom 'supporting evidence' could be found on the internet. In this tiny handful of cases the individuals had either admitted to file sharing openly on public internet forums or they had *appeared* to do so.

In at least one case the 'incriminating' post was actually made by another person using the same username. You do need to be aware of what information is available, even if you didn't put it there.

Assessing your position is a matter of working through a multitude of combinations and a web of interlinked information.

Consider this example:

Both of the following facts are true of our fictional character, Charlie:

- Charlie has *never* used his real name online *anywhere*
- Charlie has never admitted to file sharing the work in question online anywhere (not even under an anonymous username)

Neither of these facts stopped a case being prepared against Charlie - *a case which didn't exist until after Charlie read his letter and acted*. How strong that case might be considered is debateable.

Here is one more crucial fact concerning our fictional character:

- Charlie posted in a car-modification forum that he'd received a speculative invoicing letter

As far as this example goes that was enough to scupper Charlie. What you don't know is this:

- Unlike many of the people targeted in the speculative invoicing scheme our fictional Charlie did indeed illegally share the file in question.
- Charlie downloaded the file using eMule and left the file in his shared folder. It was therefore available for upload.
- When Charlie set up eMule (a couple of years ago) he entered a username into the software: 'sp4rky1989'
- This username was captured at the same time as his IP address was recorded as having the file available to upload.
- Charlie uses that same username on several forums on the internet – including his favourite: www.car-mods-r-us.com
- Until Charlie posted about the letter all the speculative invoicers knew was a username.

- Once Charlie had posted, all it took was a single Google search and they knew they had a match: a sp4rky1989 linked to the IP address evidence and now a sp4rky1989 that confirms he's received a letter.
- It's a hit! Let's sue!

All they had to do was search for the name of their own law firm plus a few keywords, click through a few forums and there he was. Sp4rky1989 was confirmed as *not just anyone* using the internet connection in question. It was confirmed as the account holder: Mr Charles Edward Baker, aged 23, of 36 Thorndyke Road, Thirsk, North Yorkshire.

Even if you don't consider that a confirmed username is sufficient to hold up in court; it's beyond debate that it provides a very strong incentive for a lawyer to do a lot more digging.

Charlie wouldn't necessarily have been any better off even if he didn't use eMule, or a similar client. Consider another scenario (which doesn't depend upon the initial knowledge of a username):

- On an internet forum Charlie had previously posted (as sp4rky1989) about a problem he'd had obtaining an exhaust from an online supplier.
- On a completely different website (under a completely different username) Charlie had previously made posts about file sharing ("I just got a new hard drive coz this one is so chokka with warez!")
- A couple of days ago Charlie posted on a website that he'd received a speculative invoicing letter.

Your first thought might be that it would be impossible to link his post about the speculative invoicing letter to anything of use. What you don't know – and what Charlie didn't think twice about was…

Charlie's profile on the site where he discussed the exhaust included a section for interests. His included an alphabetical list of bands he liked.

This same list was reproduced by Charlie in a discussion on the file sharing site.

All the speculative invoicers had to do was note the username when Charlie made his post announcing receipt of a letter. They ran a quick search on that and found the car modification site. Looking at the profile they took a guess and ran a couple of searches; they tried the text in his signature file, the exact phrasing of his location plus a few other keywords… and they tried the text of his band list.

The band list gave them a 100% match on a file sharer. A little more digging and they would find that the locality of this file sharer (which he had discussed in the forum – though not by name) shared striking similarities with Thirsk, Charlie's town. Coincidence? Possibly, but not likely.

In this example though, it doesn't need to be two internet forums and a list of his favourite music. It could have been a part number for a headlamp and a couple of internet forums; an internet forum, a corporate website and a telephone number; a single internet post and the use

of the same username; a careless registration on a website where your email address was left exposed… you get the idea.

You need to be incredibly aware of what information there is about you online, or what information *appears* to be about you. A postcode connects to several addresses, each with a history of residents. A telephone number is unlikely to have always been yours. Usernames are rarely unique across the internet.

Unfortunately the weak information used by the speculative invoicers to start these claims is not sufficient to use for anything other than threatening letters. The digging therefore begins… but if you happen to share 'personal' details with someone that *has* shared files then your job is that much harder.

Here are some other things that might've been true about a potential 'Charlie' that might not have occurred to you:

- His employer had posted details about Charlie on the company website, including the college he studied at, his job title, direct office telephone number, his interests and a rough outline of the work he does.
- A friend had posted Charlie's phone number on a social networking site when she was trying to arrange a meal out six months ago. She didn't realise her post could be seen, but the weak privacy settings of a friend who also posted in the comments left it wide open.
- The same page included masses of personal information about Charlie. This however, had marginally better privacy settings – only 'friends of friends'.
- Sam, a friend of Charlie, has 376 friends on the same site. Competitive friend, Ray, has 378. When a speculative invoicer, wanting more information on Charlie, using a fake profile, clicks to be added as Sam's friend – Sam accepts. Charlie is now wide open.
- Two years ago, Charlie sold a spare set of spark plugs online. The post contained his email address along with a whole host of other personal information.
- Five years ago Charlie posted a short review of an album on Amazon. The review shows both his 'verified real name' and one of his internet usernames.

The above lists represents a tiny portion of the personal information which might potentially be available online. You need to consider anything about you that makes you apparently identifiable – you've suddenly got a stalker, and an unpleasant, financially motivated one at that.

Did you yet consider?..

- Friends Reunited
- Archived news – be it on a school or company website or a local or regional media outlet
- Any social networking sites (consider if any of the following ring any bells: Facebook, MySpace, Bebo, Twitter, Friendster, Badoo, Buzznet, deviantART, Faceparty, Flixster, Geni, Habbo, Last.fm, LinkedIn, LiveJournal, MyHeritage, Netlog, Plaxo, Tagged, Tumblr, WAYN, MSN)
- Personal blogs
- Dating sites
- People search tools (such zoominfo.com and 123people.com)
- Internet forums

- Online reviews or comments
- Feedback posted to articles or blog posts
- Publicly viewable ‘wish lists’

What else have you forgotten about?

That’s not to say that all of these actually *will* identity you… but they could all present a problem and would need to be investigated.

If you know that you shared a file, even if it’s completely unrelated, you might be tempted to delete an incriminating post…

There are at least two well-known web archives and very probably more less well-known facilities. You can’t count on deleting information without trace from the internet.

You might think that on a (wholly unlikely) day in court you can deny an account on a file sharing website is yours…

…fine…until the prosecuting barrister asks if you’d mind signing into your email account and then asks for a ‘password reminder’ to be sent from the incriminating account. You have one new email.

Let’s put this in a nutshell:

How to Write a Letter of Denial (LoD)

Introduction

This section aims to help you write a Letter of Response (very probably a 'Letter of Denial') which will be effective. It should also guide you against some potential pitfalls and help you understand some of the content of a 'Letter of Denial' template. It goes without saying that a Letter of Denial is appropriate only if you are not responsible for (and did not authorise) the alleged copyright infringement. There is information in this document, however, which will probably be found of value even if this is not the correct response in your case.

Understand that this document is not a substitute for individual and specific legal advice, but presents a common-sense guide collated based on collective experiences and knowledge concerning the type of letter you will have received.

Before we go any further there are some important things to understand. Read each of these points carefully and take them in. *Re-read them once you've written anything you're contemplating sending as a response.* Some of them will be mentioned elsewhere in this handbook but it won't hurt to read them again.

The key points

1) The letter you have received is *technically legal*. It should not be ignored.

2) This does not mean you are obliged to pay them a penny. You are not legally obligated to pay *anything* — no court has ordered you to do so.

3) The type of evidence that it is stated they hold against you has never yet been tested in court. No one has ever yet appeared in court and lost against the company writing to you on the basis of this evidence.

4) The fact that a letter is based on a template does not stop it being legally valid. You are perfectly entitled to use a template letter and not change a single word if you so wish.

5) A template letter may not fit perfectly the needs of your own case.

6) Give as little additional information in your response as you judge necessary to create a valid Letter of Response. Do not answer questions which have not been asked.

7) The company know your address and probably your name. They have been supplied with some mysterious 'evidence' which includes an IP address which your ISP has linked to your connection. Outside of that and the name of the work they allege was shared via your connection they know almost nothing about you. Do not tell them anything you don't need to. It will not be to your benefit and may be to your disadvantage.

8) You should read the relevant part of the 'Practice Direction' for 'Pre-Action Conduct'. It's available on the internet – and in fact the most relevant section is reproduced in the appendix of this handbook.

9) You should read the letter you have been sent carefully. While they are largely mail-merged there have been subtle differences found between various letters. Letters regarding an infringement of copyright on a game, for example, can be slightly different to those claiming regarding pornography.

10) Once you've written your letter, wait for a while before you send it. Continue reading around and keeping yourself abreast of developments until a few days before you are required to reply. There are a couple of reasons for doing this:

    a. You might read something about the issue you'd not heard before and you might want to go back and alter your letter. You can't do that if it's already in the post.
    b. The slower the process is, the greater the chance is that this 'operation' will have been shut down.

11) Even if the copyright of the work was infringed via your connection have they demonstrated that *you* undertook this infringement or authorised it? It is enormously unlikely that they have. At the time of writing, no one has ever yet made known that they have received a letter where evidence has been supplied of this.

12) Even if the copyright of the work *was* infringed via your connection you are <u>not</u> obliged to sign any undertaking. Any undertaking you sign is likely to significantly increase your legal vulnerability and is not likely to be remotely to your advantage. You would be advised to seek legal advice, either through your Citizens' Advice Bureau or a recognised law firm. Negotiations with the company are <u>not</u> advised without fully understanding potential future implications. Bear in mind also, points (3) and (11) above.

13) When editing a template letter understand *why* you're changing anything you change.

The Template Letter of Denial

Now let's look at a typical template letter and see what purpose the various statements serve. This example is, at the time of writing, the most up-to-date version of the standard Letter of Denial template that most letter recipients use.

The Letter	Notes
[your name] [your address] [postcode]	
[claimant firm name] [insert mailing address here]	
[insert date here]	
Re: Letter before claim dated xxx concerning XXXXX ("the work")	Hopefully it doesn't need explaining that the strings of Xs throughout the letter need replacing with the appropriate information… but just in case – they do.

Dear Sir/Madam	
I am writing in reply to your letter dated xxxx stating that my connection was used in an infringement of copyright which allegedly occurred on the date xxxx and concerns the work "XXXXX" ("the work").	Note that the wording of this paragraph very carefully repeats only what they have claimed. If rephrased be careful to not make mention of 'yourself' (it's all about your *connection*) and be clear that the claim is 'alleged' (with no evidence as yet supplied).
You assert in your letter that the infringement was apparently traced to my internet connection. Your letter states that you have assumed that I was the person who carried out the alleged infringing acts. I do not consider that an assumption is a valid basis for a claim of liability.	Key to note in these paragraphs is that even if reliable evidence were available that established that the work had been unlawfully shared via your connection it would be next to impossible to prove that *you* were responsible for that action. Do not, however, embellish. Any speculation about open wireless, trojans etc is entirely irrelevant at this stage. *They* have to show that, at least in the balance of probability, *you* are legally responsible for the copyright infringement. Don't feel the need to prove their case for them, or put words into your letter that they may turn against you, or use as an excuse to write your more letters. In accordance with pre-action conduct (Section 2.1(2) of Annex A of the Practice Direction – you can find it in the appendix of this handbook) their letter ought to have stated the basis on which their claim is made (i.e. why they claim you are liable). They have failed to state why you would be liable if such an infringement had indeed occurred (because, if you didn't do or authorise it, *you're not*).
Nevertheless, I categorically deny any offence under sections 16(1)(a) or (d), 17 or 20 of the Copyright Designs and Patents Act 1988 ("the Act"). I have never possessed a copy of the work in any form, nor have I made a copy, nor have I distributed it, nor have I authorised anyone else to distribute or copy it using my internet connection or computer. I note that section 16(2) of the Act requires a person to either directly infringe copyright, or authorise someone else to do so. I have done neither, and you have not provided any evidence of my doing so.	If you are sure that you have not illegally infringed the copyright of this work then this paragraph makes this explicit. It doesn't hurt to point out, as in the final sentence, that they have provided no evidence that you have infringed their copyright. Depending on your exact situation this section may require editing. Some people receiving letters of claim have purchased and own legitimate copies of the works about which they have received letters. As such you would not claim you have never possessed a copy of the work! Do be sure of what you are, or are not, denying. Check the CDPA online; it's easy enough to find and actually fairly understandable for an Act of Parliament. Do not admit anything unlawful in this section. If you need to do that, seek legal advice. If parts do not apply, simply omit them.

Furthermore I note that, under section (16)(3) (a) of the Act, copyright is only infringed if the restricted acts are carried out in relation to the whole or any substantial part of the work. You have not provided any evidence that such an infringement has actually taken place.	It is not at all certain that an infringement of copyright of the work has actually occurred. Even if the work had indeed been shared, unless the sharing was of at least a 'substantial part' then it would not constitute an unlawful act. They have *not even tried* to demonstrate how much of the work they allege was shared – almost certainly because they do not know.
If you wish to continue to assert that an infringement has taken place then, in accordance with my entitlement as a part of pre-action procedure, I formally request a copy of any report, spreadsheet or data you hold which demonstrates that such an infringement took place via my connection or computer (including what substantial part of the work was involved, or if it were the whole) and any information gathered as to with whom the work was successfully shared via my connection (and the extent to which it was shared in each instance, if there were more than one).	Following on from the above you invite them (if they wish to continue to pursue their claim) to provide evidence that the whole or a substantial part of the work was copied or shared. Since their monitoring is via the internet, the 'copying' of the work onto a computer is an assumption – all they could *hope* to monitor would be the amount shared online. The reason for querying with whom the work was allegedly shared is that the monitor can only record how much of the work was shared from a particular IP address with *itself*. In fact, it's unlikely that even this takes place; generally the monitoring relies on snapshots of a single second showing which connections are apparently 'offering' a particular file. However, even if an entire copy of the work actually ever were shared with the monitor, no 'damages' would occur from that infringement. No sales of the work could be claimed to be lost as a result of sharing a copy of the work with a data collector employed by the copyright owner. The documents you have requested should be supplied by them "within as short a period of time as is practicable" (as required by paragraph 5.1 of Annex A of the Practice Direction).
You have requested that I supply you with the details of "the other parties at [my] residence using [my] internet connection to make the Work available for download". As you seem to be perfectly aware, it is impossible to link an IP address to a particular person or computer without further detailed analysis which requires a level of expertise I do not possess. I am told that the delay in your	Hang on!? They have a forensic computer analyst, cutting-edge bespoke software and a court order and they don't know who did it? How are *you* supposed to know? You can't even be certain that anyone's copyright has actually been infringed, let alone who did it. So you tell them that.

sending of a letter and the reality of domestic router technology would, in any case, preclude any such analysis. I have no basis on which I could assert that any individual has used my connection or my computer unlawfully to infringe your copyrights. I am not, therefore, able to provide any details in that regard.	
Your failure to supply any evidence in support of a valid claim under the Act means that there is little to answer. Simply, you have asserted that an infringement took place which I did not carry out or authorise, and you have provided no evidence to support any assertion to the contrary. I do not have the expertise to provide a detailed explanation. As such I can only conclude that I have been a victim of foul play.	Pre-action procedure says that you ought to *"give reasons why the claim is not accepted, identifying which facts… are disputed, and the basis of that dispute."* This paragraph in essence, points out that while you wish to deny the claim, you cannot provide substantive 'proof of innocence' (and indeed you should not try!). No evidence has been supplied and as such, and given your knowledge that you have not contravened the CDPA 1988, you can only state that whatever leads them to think you are responsible, is incorrect.
As far as I am aware, there is no law in the UK under which you could properly hold me responsible for an infringement occurring via my internet connection, without either my knowledge or permission. I would be interested to hear your legal basis for attempting to do so.	This points out to them that in fact they cannot hold you legally responsible for this alleged copyright infringement and challenges their basis for doing so. When their next letter to you fails to answer this point it exposes a monumentally large weakness in their claim.
Please be aware that that if you do choose to pursue this matter, I will seek to recover all my costs to the maximum permitted by the Civil Procedure Rules.	If the case were ever to go to court (a highly unlikely occurrence based on the history of this saga), this makes it clear that in the event that their claim were unsuccessful you would be seeking to recover any losses incurred during the entire process including for your time and money in responding to their letter of claim. This is limited by law, so don't bandy about random figures.

The signature of the undersigned confirms the statement provided to be accurate and legally binding under the terms required by pre-action procedure in civil law.	This makes it apparent that your letter intends to comply with the Practice Direction for Pre-Action Conduct – as it should.
Yours faithfully [name]	The letter should be signed to make it legally binding.

Some further pointers:

Do not use offensive language or angry emotive language. For example, you may be 'upset' or 'disturbed' by their letter, but avoid being 'outraged'.

Do not make threats (particularly empty threats) or promises.

Be truthful.

Do not expose ideas to them that might form the basis of your defence if you were to go to court.

Do not libel the company. If you *must* make comment on the professionalism (for example) of the companies or people involved (which is ill-advised in any case) make explicitly clear in your wording that this is *your personal opinion*. This is particularly pertinent if your letter is to be seen by third parties, for example if you decided to send courtesy copies of your letter to a consumer or regulatory body.

Do not make any kind of 'offer' without first taking legal advice or being *exceptionally* sure what you are undertaking.

If they have made inaccurate observations in their letter it is unlikely to hurt your case to record these in your letter (for the benefit of any future court proceeding). For example, if they have made reference to an enclosure which was not supplied; point this out.

If you pay to make the letter 'go away' this may well be used as evidence against you in any potential future claims. At present the strength of their evidence has never been contested in court. It is likely that a payment received in settlement from yourself for a prior claim would be stronger evidence on a future claim than any mysterious 'evidence' which they state their client holds.

About your second (and third, and fourth?) letters…

You will, unless the operation has already been shut down, very probably receive, in due course, a second letter. The same thinking applies to writing that letter:

- Minimal content
- Straightforward repeat denial

- Note the lack of evidence; and observe that they have only reasserted their claim of the first letter
- Note that you find their letters threatening and harassing. Warn that future correspondence will be considered harassment.
- Repeat that you will seek to fully recover your costs in the event of court action
- Again note that your letter is written is accordance with pre-action procedure (the Practice Direction for Pre-Action Conduct)

You still **do not pay**.

Sometimes a questionnaire is sent requesting further information. If they do ask for information then the following paragraph may be useful:

> "I shall not be answering your questionnaire. If there is such uncertainty in the matter of your claim and its evidentiary basis that you feel the need to send me a questionnaire, I would respectfully suggest that you might usefully review the basis for these claims and the way you go about selecting the individuals of whom you make demands for settlement."

You still **do not pay**.

I'm thinking about paying to settle

Really? Crumbs.

Okay, well, here's some additional advice:

Be really, really sure about what you're doing and getting into. Paying is not the 'easy way out'.

Next up: 'without prejudice'. The term 'without prejudice' is used in the course of legal negotiations to indicate that a particular conversation or letter cannot be tendered as evidence in court. Any letter in which you offer any kind of settlement should certainly be titled 'without prejudice' so that it cannot subsequently be used against you in court.

Be aware that it is not necessary to admit liability or to sign any undertaking in order to offer a settlement. Frequently firms and individuals will offer settlement as a 'gesture of goodwill' to conclude proceedings. The same option is open to you if you decide that settlement really is the way forward for you.

Understand what constitutes an appropriate level at which to settle and be prepared to walk away if the settlement offered is unacceptable or inappropriate. Because of the way peer-to-peer file sharing works it is not possible for the average amount of any file shared by any peer (person sharing the file) to be greater than *a single copy*; quite often it might be less.

Think of it like hugs; you can't give one unless someone wants it. No one within the swarm needs more than one copy; therefore no person within the swarm can share, on average, more than a single copy. Any settlement you propose, or which is offered to you, in the event that you are responsible, should reflect this.

Appendix

Practice Direction for Pre-Action Conduct: Annex A

The relevant section of the Practice Direction for Pre-Action Conduct is reproduced on the following pages in accordance with the Open Government Licence for Public Sector Information (http://www.nationalarchives.gov.uk/doc/open-government-licence/)

The entire document can, at the time of writing, be found here: http://www.justice.gov.uk/courts/procedure-rules/civil/pdf/practice_directions/pd_pre-action_conduct.pdf

ANNEX A

GUIDANCE ON PRE-ACTION PROCEDURE WHERE NO PREACTION PROTOCOL OR OTHER FORMAL PRE-ACTION PROCEDURE APPLIES

1. General

1.1 This Annex sets out detailed guidance on a pre-action procedure that is likely to satisfy the court in most circumstances where no pre-action protocol or other formal pre-action procedure applies. It is intended as a guide for parties, particularly those without legal representation, in straightforward claims that are likely to be disputed. It is not intended to apply to debt claims where it is not disputed that the money is owed and where the claimant follows a statutory or other formal pre-action procedure.

2. Claimant's letter before claim

2.1 The claimant's letter should give concise details about the matter. This should enable the defendant to understand and investigate the issues without needing to request further information. The letter should include –

(1) the claimant's full name and address;
(2) the basis on which the claim is made (i.e. why the claimant says the defendant is liable);
(3) a clear summary of the facts on which the claim is based;
(4) what the claimant wants from the defendant;
(5) if financial loss is claimed, an explanation of how the amount has been calculated; and
(6) details of any funding arrangement (within the meaning of rule 43.2(1)(k) of the CPR) that has been entered into by the claimant.

2.2 The letter should also –

(1) list the essential documents on which the claimant intends to rely;
(2) set out the form of ADR (if any) that the claimant considers the most suitable and invite the defendant to agree to this;
(3) state the date by which the claimant considers it reasonable for a full response to be provided by the defendant; and

(4) identify and ask for copies of any relevant documents not in the claimant's possession and which the claimant wishes to see.

2.3 Unless the defendant is known to be legally represented the letter should –

(1) refer the defendant to this Practice Direction and in particular draw attention to paragraph 4 concerning the court's powers to impose sanctions for failure to comply with the Practice Direction; and

(2) inform the defendant that ignoring the letter before claim may lead to the claimant starting proceedings and may increase the defendant's liability for costs.

3. Defendant's acknowledgment of the letter before claim

3.1 Where the defendant is unable to provide a full written response within 14 days of receipt of the letter before claim the defendant should, instead, provide a written acknowledgment within 14 days.

3.2 The acknowledgment –

(1) should state whether an insurer is or may be involved;

(2) should state the date by which the defendant (or insurer) will provide a full written response; and

(3) may request further information to enable the defendant to provide a full response.

3.3 If the date stated under paragraph 3.2(2) of this Annex is longer than the period stated in the letter before claim, the defendant should give reasons why a longer period is needed.

3.4 If the defendant (or insurer) does not provide either a letter of acknowledgment or full response within 14 days, and proceedings are subsequently started, then the court is likely to consider that the claimant has complied.

3.5 Where the defendant is unable to provide a full response within 14 days of receipt of the letter before claim because the defendant intends to seek advice then the written acknowledgment should state –

(1) that the defendant is seeking advice;

(2) from whom the defendant is seeking advice; and

(3) when the defendant expects to have received that advice and be in a position to provide a full response.

3.6 A claimant should allow a reasonable period of time of up to 14 days for a defendant to obtain advice.

4. Defendant's full response

4.1 The defendant's full written response should –

(1) accept the claim in whole or in part; or

(2) state that the claim is not accepted.

4.2 Unless the defendant accepts the whole of the claim, the response should –

(1) give reasons why the claim is not accepted, identifying which facts and which parts of the claim (if any) are accepted and which are disputed, and the basis of that dispute;

(2) state whether the defendant intends to make a counterclaim against the claimant (and, if so, provide information equivalent to a claimant's letter before claim);

(3) state whether the defendant alleges that the claimant was wholly or partly to blame for the problem that led to the dispute and, if so, summarise the facts relied on;
(4) state whether the defendant agrees to the claimant's proposals for ADR and if not, state why not and suggest an alternative form of ADR (or state why none is considered appropriate);
(5) list the essential documents on which the defendant intends to rely;
(6) enclose copies of documents requested by the claimant, or explain why they will not be provided; and
(7) identify and ask for copies of any further relevant documents, not in the defendant's possession and which the defendant wishes to see.

4.3 If the defendant (or insurer) does not provide a full response within the period stated in the claimant's letter before claim (or any longer period stated in the defendant's letter of acknowledgment), and a claim is subsequently started, then the court is likely to consider that the claimant has complied.

4.4 If the claimant starts proceedings before any longer period stated in the defendant's letter of acknowledgment, the court will consider whether or not the longer period requested by the defendant was reasonable.

5. Claimant's reply

5.1 The claimant should provide the documents requested by the defendant within as short a period of time as is practicable or explain in writing why the documents will not be provided.

5.2 If the defendant has made a counterclaim the claimant should provide information equivalent to the defendant's full response (see paragraphs 4.1 to 4.3 above).

6. Taking Stock

6.1 In following the above procedure, the parties will have a genuine opportunity to resolve the matter without needing to start proceedings. At the very least, it should be possible to establish what issues remain outstanding so as to narrow the scope of the proceedings and therefore limit potential costs.

6.2 If having completed the procedure the matter has not been resolved then the parties should undertake a further review of their respective positions to see if proceedings can still be avoided.