

Warning notice

Warning notice

Bogus law firms and identity theft

Bogus law firms and identity theft

Updated 25 November 2019 (Date first published: 26 March 2012)

Status

This document is to help you understand your obligations and how to comply with them. We may have regard to it when exercising our regulatory functions.

Who is this warning notice relevant to?

Consumers of legal services and those we regulate.

Our concerns

1. There are serious and continuing risks to the public arising from the activities of criminals and criminal gangs who set up bogus law firms or bogus branch offices of genuine law firms. This is with the intention, usually, of stealing money, personal information or data. This warning notice provides information about the threat as well as advice about how to protect yourself and others from it.
2. We are using our resources to mitigate the risk in various ways including rigorous authorisation processes, use of intelligence, urgent investigation, removal of records from the Digital Register and publication of warnings
[<https://www.sra.org.uk/consumers/scam-alerts/>] .
3. It is important to bear in mind that we do not regulate the people who are perpetrating these frauds and our powers over them are relatively limited.
4. It is important to share some of the indicators of these frauds to maximise the chances of prevention.
5. If you become suspicious about a law firm for any reason, please contact us [<https://www.sra.org.uk/contactus>] as a matter of extreme urgency since some frauds are carried out very quickly.



6. Bear in mind that you may come across these frauds in different contexts. You should keep an eye on any indication that a firm is being targeted or its name being used improperly. If you discover this, you should contact us immediately.
7. Some examples of factors that may give rise to suspicion are¹ [<https://www.sra.org.uk/solicitors/guidance/bogus-law-firms-identity-theft/#note-1>]
 1. errors in letterheading — for example misspelling the name of the town in which a firm or office is supposedly based
 2. no landline telephone number — note that numbers beginning with 07 are mobile telephone numbers
 3. inconsistent telephone or fax numbers with those usually used by the firm
 4. telephone calls being diverted to a call-back service
 5. a firm apparently based in serviced offices
 6. email addresses using generic email accounts, eg gmail — most law firms have addresses incorporating the name of their firm. If in doubt, check the genuine law firm's website to identify its contact email address. You may well notice a difference
 7. sudden appearance in your locality of a firm with no obvious connection to the area, probably not interacting with other local firms at all
 8. a firm appearing to open a branch office a considerable distance from its head office for no obvious reason
 9. a firm based in one part of the country supposedly having a bank account in another part of the country — this is a strong indicator and has been seen several times
 10. a client account apparently overseas — this is a breach of rule [<https://www.sra.org.uk/solicitors/handbook/accountsrules/part4/rule13/content>] and is a major red flag
 11. a firm's website which does not display the SRA's clickable Logo—all firms regulated by the SRA must display the SRA's clickable Logo on their website (see rule 1 of the Transparency Rules)
 12. a strange or suspicious bank account name — such as the account not being in the name of the law firm you are supposedly dealing with either at all or by some variation.



8. This list is not exhaustive. Nor does the presence of one of the factors on it mean that you are dealing with a bogus law firm or solicitor. However, where you see the factors above you should act cautiously and take steps to safeguard your position.
9. If you become concerned, because of the possibility of the theft of the identity of a genuine solicitor, it is worth trying to speak to the solicitor concerned. For example, if the solicitor is supposedly at one particular office but is also based at a head office of the firm, you could speak to the head office preferably after verifying its genuine nature, perhaps by contact with the senior partner.
10. You should check whether the firm's website displays our clickable logo. Not all firms are regulated by us, but most are. All firms which the SRA does regulate must display our clickable logo. However, presence of a clickable logo should not be taken as proof that a website is genuine. A fraudster may have copied a genuine image and displayed the copy on their website. More information on how you should use the clickable logo is available
11. You should check our digital since there are sometimes bogus law firms which have not sought registration with us and will not appear there; but bear in mind that the nature of identity theft is that fraudsters may have obtained some form of registration by fraudulent misstatement to us and therefore an entry on the digital register should not be taken as verification that the firm is genuine.
12. If you are sending money to a firm, we suggest you send a small amount first and then speak to someone you have been dealing with at the firm to ensure they have received it, before you send the rest of the money.

Our expectations

13. We encourage everyone to be vigilant for warning signs that a solicitor or firm's identity may have been stolen.
14. It is important that you report your suspicions to us immediately.
15. If you are an owner or manager of a law firm and you suspect your firm is being targeted or its name is being used improperly, as well as contacting the us, you should also contact your insurers and consider legal action (such as applying for an injunction) either to stop misleading statements or to freeze assets if money has gone missing. If



there is any evidence of a crime having been committed, you should also inform the police.

16. There are risks to you and your firm, as found in *Lloyds TSB Bank PLC v Markandan and Uddin* [2012] EWCA Civ 65 where the firm that was said to be the victim of the fraud was still held liable for breach of trust in paying away mortgage monies.
17. If you are an owner or manager of a firm, there are some practical things you can do:
 1. Search your firm's name on the internet from time to time, since that might bring up details of a false office or false contact details for your firm — it may be worth considering doing the same with the names of some of your partners or staff
 2. Check your firm and individual details on the SRA Digital Register—in case someone has misused your name to set up a false office
 3. Be alert to suspicious incidents such as transactions that others seem to think your firm is dealing with when you are not
 4. Look out for alerts and warnings on our website about bogus firms
 5. Never send details of a change of bank account to your clients by email.
18. Do not assume that we or the police can take direct steps to protect your firm. We each will do what we can although we will be focused on fraud prevention and you must not exclude the possibility of urgently seeking an injunction particularly if you are in possession of the most direct evidence and indeed if action is required very urgently. In such circumstances, we will seek to assist as much as we properly can in light of the evidence and any order of the court.

Further help

If you require further assistance, please contact the Professional Ethics helpline [<https://www.sra.org.uk/contactus/>] .