Cyber-crime is on the increase, and you should be on the look-out for it to ensure that you do not become a victim of it. The website of the Solicitors Regulation Authority contains a 'Scam Alert' database which provides members of the public with information about known scams in which the identity of a legitimate law firm or a legitimate lawyer has been used by persons unknown for what are assumed to be criminal purposes (www.sra.org.uk).

You should be alive to the possibility that a fraudster might deliberately misrepresent himself or herself as a member of, or as someone acting on behalf of or working with, this firm for criminal purposes. Such scams normally originate by email. Often the email will either promise the recipient a share of a large sum of money in return for paying a modest sum up front (an advance fee type fraud) or request personal or financial information about the recipient or the recipient's bank account allegedly in order that money can be paid to them (an identity theft type fraud). In an attempt to give legitimacy or respectability to the scam, sometimes the email will direct the recipient to a false website that intentionally replicates the look of a legitimate website (a cloned website).

The website of this Firm may be cloned by persons unknown using web hosting companies located abroad for what we believe are criminal purposes, and from time to time scam emails may be in circulation which purport to come from this Firm or a Firm member or from a bogus firm or bogus lawyer with a name which is similar to but not identical to the name of this Firm or a Firm member.

The scam emails often inform the recipient either that lottery winners wish to donate money to them, they might be a beneficiary of the estate of a deceased person or they might be the beneficiary of a recently discovered life insurance policy. Such emails are invariably fraudulent and should not be replied to or acted upon unless or until their provenance can be established. If you receive an unsolicited and poorly worded email from someone you do not know who is using a free email service and an unusual email address and it contains information or an offer which appears too good to be true, it very likely is not true.

If you receive an email purporting to come from this Firm or a member of the firm, or if you are directed to a website which purports to be the Firm's website, and you have doubts or concerns about the provenance of the email or website, before taking any action please either contact the Firm member you normally deal with or email the [ ] [email address] and s/he will tell you whether the email came from us or whether it is our website.