SoA GUIDANCE NOTE 2024

Scams

Guidance notes can give only a brief, generalised overview and the SoA cannot give legal advice. Members are always welcome to consult the SoA for bespoke advice. We try to keep the guides up to date but if you spot errors or omissions, please let us know by emailing info@societyofauthors.org marked 'Guides feedback'.

Beware of Scams

The internet is teeming with companies offering services to authors, and it can be difficult to distinguish between legitimate offers and scams. Always treat information sourced from the internet, or from cold-call emails, with great caution, and remember that scams are designed to play on your hopes as an author.

In the last year, we have seen a variety of misleading unsolicited offers and cold-calling:

To act as the author's agent – they may claim that they are the authorised scout for specific (real) publishers or were the agent for a specific (real) book or famous author, they sometimes use the name of a (real) agent, or say a specific (real) publisher has expressed interest in the author's work. All are lies.

To publish the author's book – sometimes seemingly for free or for 100% royalties. Don't be fooled. If it looks too good to be true, it almost certainly is.

To ghostwrite. One such scammer then aggressively pressed also to publish and publicise the author's work, all for further fees.

To boost ebook sales, increase income from Amazon, or manipulate Amazon's rankings. Such sites often give the strong impression that they are Amazon companies, affiliated with Amazon, or are Amazon-endorsed. They are not.

To mentor or help authors write a screenplay and attract the attention of producers.

The fallout can be distressing. SoA members have reported that:

They have paid for services but cannot recoup the money they have spent.

They are left disappointed, sometimes demoralised, about being misled. Many feel that they have been made a fool of. Not true. This isn't your fault – these people are extremely clever at what they do.

They have given away rights in their works that they cannot get back.

In a couple of instances, they were pressured by excessive follow-up emails and phone calls – an approach similar to persistent bank scammers who repeatedly request your login details because someone is, as we speak, 'spending thousands of pounds on your credit card in Harrods'.

Things you can do to minimise the chance of being scammed

Check with the SoA. If the offer is bona fide, it will be a pleasant surprise.

Take your time and do not rush into answering flattering emails or sharing your work. Scammers sometimes use email addresses that look like a genuine publisher's address. Remember that publishers and producers are highly unlikely to make spontaneous offers or try to acquire rights in books that have not been submitted to them.

Do not rely on glowing reviews that you find online. Your search is likely to bring up only results curated by the scammer's paid advertisements and not always independent positive comments. Instead, search for 'is it a scam?' or 'is it legit?'.

See https://writerbeware.blog/scam-archive/ (but remember that it is not an exhaustive list).
See also https://writerbeware.blog/2023/12/15/how-to-spot-a-fake-literary-agency/.

Never pay money unless you are clear about what you will receive in return. Don't settle for vague promises and aspirational jargon, but only for specific undertakings. Ask the SoA to vet the contract you are offered.

Remember that legitimate Amazon websites contain 'amazon.co.uk' or 'amazon.co.uk/support'. Anything else and it's not Amazon.

If the scammer cites a genuine agent or publisher, report the matter to that agent or publisher (most big publishers have a 'report a scam' link which can be searched for online). Publishers and agents routinely bring legal action against such scammers.

Links which may be of interest

Overseas Scams – Writer Beware (bear in mind this is not an exhaustive list).
https://authorsguild.org/news/beware-of-publishing-scams/
https://www.penguinrandomhouse.com/prh-fraud/#phishing-scam-alert
https://www.gov.uk/report-suspicious-emails-websites-phishing
The American Booksellers Association suggests that 'the recipient should definitely report the email as spam/phishing/fraud to their email provider. This could also be wire fraud which is handled by a variety of [US] agencies, but the person could start at https://reportfraud.ftc.gov/#/.'

Some other 'bad actors'

Prizes and grants:

We hear reports of scammers pretending to be the legitimate beneficiary/prize-winner and insisting that the grant or prize money be sent to the scammer. They can be very convincing. If you are awarded money, contact the official prize administrators via the contact information on their website at an early stage and ask them to take rigorous precautions to ensure that they send the money to the right person.

If you receive an unexpected email saying you have won a prize or been awarded a grant, contact the organisation (by its regular email or phone number) to check that it is bona fide.

Payments and statements which should be coming to you from publishers or other companies:

One author reported that payments from three different sources never appeared in their bank account. When they pursued the matter, each of the payers said they had been given authority to make payments to a new account. In another instance, a member believed they were paying money owed to a specific (legitimate) company, only to discover they were in fact paying a scammer. In both cases, securing refunds was time consuming and complex.

How to spot that you (or your publisher) might have been scammed

Always be careful before acting on emails or phone calls purporting to be from your bank, even if the caller ID that appears on your phone matches your bank name or number. Scammers can change the number that appears on your screen. Remember that banks will never ask you to disclose details about your account or security code details over the phone, and will always ask security questions of you before talking to you.

As soon as you receive a royalty statement or know a payment is due (e.g. an instalment of the advance), check that the statement is correct and that the payer has your correct bank details. Note when the payment is to be made and check to ensure that it has been received in your or your agent's bank account.

Chase immediately if the expected money has not been paid.

We recommend setting up a two-step verification system with your agent or publisher which they must use in the event of a request to change personal or financial details on their system, for instance a letter and a phone call quoting a prearranged identity question.

If you make regular payments to other parties, be wary of any request to transfer the monies to a different account and ensure (by some means other than email or by going via any contact details supplied with the request to change bank details) that the request is bona fide.

We understand that if a PayPal payment for any reason goes to the wrong person, you may have no redress. So bear this in mind, especially for any sizeable payment.

Publishers, agents, and indeed, everyone is now required to take steps to keep people's personal data and confidential information safe, and a data leakage to a scammer could have serious consequences under the Data Protection Act – yet another reason to always be ultra-cautious when giving out your – let alone anyone else's – contact and other personal information.

What you can do if you have been scammed

If money has been taken from your bank account without permission, whether your identity has been stolen, your card cloned, there is unfamiliar activity on your account or you've been the victim of a scam, there are certain steps you should take.

See the Money Advice Service and note the three contact links advised in the guidance.

Alert your bank or card provider. You could be liable for all money lost before you report it.

Contact Action Fraud to report the crime if you've been scammed. This can be done online or by calling 0300 123 2040. You can also report financial scams, such as investment fraud, to the Financial Conduct Authority (FCA).

If a scammer has taken money from your own bank account, it will generally be your responsibility to pursue the matter (if you can), but you may be able to reclaim it if you have taken proper precautions – see the guidance above.

If a scammer has diverted money from its originally authorised destination through no fault or negligence of the real recipient, the responsibility generally lies with the payer. Let's say a publisher or producer sends regular payments to you; then a scammer contacts the publisher/producer, pretending to be you, notifying them of a change of account and asking that future payments should go to 'your' new (i.e. the scammer's) account. As well as enriching the scammer, it means that you have not been paid. Our understanding is that – unless the error was caused by your gross negligence – you are entitled to look to the payer for the money you are still owed. It would be up to the payer to pursue compensation for the fact that it had wrongly sent money to a fake account. Contact us if you are experiencing difficulty in convincing a publisher or other payer to pay you.

In practice, taking action to recover monies (from the original payer or, in the payer's case, from the bank or via the courts) in such an event can be complicated and slow. It is in everyone's interests to spot fake accounts as early as possible and to reduce the risk in the first place.
For more information, see Warning: Misleading Invoices – Gov.UK.