

Vacation Rental Scams Targeted To Vacation Home Owners

The following guide is to caution property owners of the types of correspondence that have been linked to fraudulent activity.

1. Potential indicators of suspicious emails

Telling signs of a fraudulent email include poor grammar, irregular usage of capitalization, over earnest attempts to guarantee that the payment method is legitimate, use of title or profession to indicate or act as a guarantee of financial status (e.g. government official, doctor or similar) along with other attempts to provide superfluous or irrelevant information as a means to impress the exigent or 'out of the ordinary' rationale behind a delayed or overpayment.

It is important to note that initial correspondence may initially appear to be legitimate; however, as correspondence begins to focus upon means of payment, indicators of suspicious activity may become more apparent. Significantly, fraudsters can work as a network, hence when one or more parties are referred these too may be part of the fraudulent network. Lastly, fraudulent parties will endeavor to use the most effective and 'naturalistic' method to extort money from property owners, and will inevitably have access to the below information, as such it is important to be as vigilant as possible if you ever become suspicious of correspondence from a potential renter.

2. Types of Fraudulent Activity

Overpayment

The fraudulent party makes an initial payment in excess of the requested total for the accommodation by a payment method which can take several days or longer to clear into the property rental owner's account. In the meantime the fraudulent party requests for the excess to be repaid by direct bank/wire transfer. By the time the excess has been paid, it becomes apparent that the initial payment was a fraudulent transaction which will not clear. We recommend that property owners always endeavor to avoid collecting excess payments for agreed accommodation. In the event that they choose to make a return payment, always ensure that the original payment has completely cleared into your account by contacting your bank.

Please note that depending upon where the transaction has originated and the skill of the fraudster that it may take more than a month before payments such as cashier checks, travelers checks, certified checks, personal checks or otherwise are identified as forgeries.

Whether fraudulent or not, please be wary of transactions from non-Western nations where payment may take longer to process than usual payment types.

Please consult your local bank for confirmation of typical payment clearing schedules.

Please be aware that many banks may show a payment as credited to an account before the payment has fully cleared. If in doubt, always clarify with your bank that the payment has completely cleared before accepting any payment.

A preferable solution to the situation is to cancel the initial transaction and request a replacement payment for the correct amount due.

Indirect Overpayment

Variations of the above scam include attempts alternative attempts to send an overpayment to the property owner. This may take a number of guises, and as outlined above, property owners should be very cautious of ever accepted any form of overpayment.

Common methods of overpayment include requests to accept payment for the fraudulent party's car hire, tour excursions, wedding gift, honeymoon surprise or similar - either directly from the fraudulent party or a third party relation, i.e. spouse, employer, parent etc.

The fraudulent party makes payment by delayed payment process such as a check and then follows up with correspondence that the excess payment is no longer needed and requests that the excess payments are refunded immediately, before the initial payment by the fraudulent party has cleared.

The fraudulent party may also proceed to become aggressive or threatening in nature, requesting immediate repayment and even threatening legal action.

Again, a preferable solution to the situation is to cancel the initial transaction and request a replacement payment for the correct amount due. Inform the renter that you will only accept payment for the exact amount due that all payments must clear prior to renting your property.

Acquiring Bank Details

Property owners are advised to never release confidential payment information to any third party requests no matter what. There is never a justifiable reason for a property owner to release confidential payment information, and in the event that a transaction needs to be identified for whatever reason a payment reference will always suffice. Following from the above indirect overpayment scam, the fraudulent party may claim that they are uncomfortable releasing their payment details to the second party service provider from overseas as they are not 100% certain of their reliability/ would feel happier only releasing their payment details to one party, and as such would feel more comfortable if the property owner proceeded to pay the service provider on their behalf.

In order for the second party service provider to identify their payment (as it will be coming from a different source) the fraudulent party may ask for the property owners payment details - allegedly to help the service provider identify the fraudulent party's transaction.

Alternatively the fraudulent party may request to wire the money directly into the property owners account, however, request excess confidential payment information such as account numbers, social security numbers or otherwise. If you are ever in doubt as to what information is legitimately required to complete a wire or bank transfer into your account, always consult with your local bank directly for further advice.

3. General

In the event that you receive suspicious correspondence, we advise against entering into any further correspondence. If the fraudulent party has already made payment and you are uncomfortable proceeding for whatever reason, cancel the payment immediately and avoid further correspondence. If you believe that you have received a fraudulent payment, we recommend reporting the transaction to your local crime prevention unit who will be able to take the necessary procedures to follow up the transaction.

FTC toll free hotline: 877-FTC-HELP (877-382-4357)

FTC online complaint form (www.ftc.gov)

Internet Fraud Complaint Center (www.ic3.gov/)

Non-emergency number for your local police department.