Virtually squatting – typologies and preventative measures

Extract from NCA Amber ALERT of June 2024 (Reference 0742 - NECC)

Overview

The purpose of the alert is to is to summarise the threat of virtual squatting and to aid entities in spotting virtual squatters, as well as providing tools to help regulated entities protect themselves from being exploited by this typology.

Introduction

Virtual squatting is where those committing economic crime attempt to create legitimacy to their activities, create anonymity, or evade investigation, by registering their company or legal entity at the addresses of serviced offices, accountants and law firms without consent, or legal agreement, to do so. The false information supplied to Companies House may enable criminals to access financial products or other benefits.

Law enforcement and supervisory authorities have identified that this could be a widespread problem and virtual squatting increases the vulnerability of the regulated sector to being exploited by those using this typology – since the criminals will look to exploit the addresses of the regulated sector to provide the veneer of respectability and legitimacy.

The victims of virtual squatting (i.e. those whose addresses are being used without consent) may be affected by adverse impact on their reputation. This may occur through unfair association with the criminal groups and could result in the regulated entity / regulated sector from experiencing lack of trust by the wider economic crime system.

Virtual squatting is a key typology for fraud – with investment fraud, mortgage/financial product fraud, or government support fraud being enabled through criminals falsely registering businesses at unconnected addresses.

The use of serviced offices and mail forwarding business to enable fraud was first identified via investment fraud. Many criminals recognised the benefit of having an address in the City of London and wanted to exploit this association, and address, in their marketing material. However, the fraudulent businesses are not physically present at their registered office. More recently, crypto-currency fraud has utilised virtual squatting.

This typology has also been used to commit:

- government support scheme fraud (such as Bounce Back Loan fraud) with companies set up to apply for government financial support during the COVID pandemic using false addresses, and then quickly ceased once the funds were extracted from the company bank accounts;
- VAT fraud by overseas sellers on online trading platforms (see BBC article); and
- identity theft, allowing fraudsters to access finance products in the name of the individual whose identity has been stolen.

Company addresses

An appropriate registered office address is required when setting up a limited company. The registered office address is the company's official address and can be separate / different to the principal place of business of the company.

An address is an 'appropriate address' if, in the ordinary course of events:

- a document addressed to the company, and delivered there by hand or by post, would be expected to come to the attention of a person acting on behalf of the company
- the delivery of documents there is capable of being recorded by the obtaining of an acknowledgement of delivery.

The company address will be publicly available on the online register. The company cannot remove the address from the register.

If the company directors do not want an address to be publicly available (for example, if it's a home or someone lives there) the company can either:

- use a different address, such as the address of professional advisor; or

- appoint an agent
- who will give you an address to use.

The company must have permission to use the different address.

Case study

A professional services firm identified an increase in virtual squatting, with squatters becoming more targeted. For example, not only does the firm get companies moving their registered office to the firm's address without its knowledge or consent, the firm had found that squatters were looking at actual clients' names and then setting up a company with a name which looks very similar, for example AB Partners Ltd and AB Paartners Ltd.

How regulated businesses can protect themselves from exploitation

Identifying the misuse of the address is relatively easy – the quickest way is to input the regulated businesses' postcode and property number/name in the advanced search function on the Companies House website (Advanced company search - Find and update company information - GOV.UK (company-information.service.gov.uk), which will bring up the names of all those who are registered at the address (filter for active companies rather than "all").

Regulated entities should regularly check to see which companies use their address as a registered office. Many of these may be legitimate businesses if the regulated entities are providing registered office services as a Trust and Company Service Provider (TCSP). However, if the regulated entity does not recognise a company name, and this is not because of a name change or the registration of a new subsidiary of an existing client, the regulated entity should take action to correct the Register to stop being associated with criminal activity.

If there are contact details for the directors or the entity itself (other than the incorrect registered address), the regulated entity should consider contacting the director/company to request that they change their registered address.

If this is unsuccessful, or if there are no other contact details, the regulated entity should apply to Companies House to change the address. The application can be made on the Companies House website: Apply to change a company's disputed registered office address (RP07) - GOV.UK (www.gov.uk)

As part of the process, Companies House will write to the Company and its officers to ask them to update the address. If the company does not change the address after 14 days, Companies House will change the registered office address to a Companies House default address. This is the best available action as, currently, Companies House does not have the powers to remove a registered office address from the Companies House register.

Tools to identify virtual squatters via customer due diligence (CDD)

As part of enhanced due diligence (at either take-on or during ongoing monitoring), regulated entities may wish to perform additional procedures to confirm the address of a corporate entity, or the principal place of business, if they have identified risks or red flags about a potential, or existing, customer.

In this section, we set out resources and information that may assist the regulated entity in verifying whether a registered office is legitimate.

Red Flag Indicators

The Virtual Squatting cell members identified the following red flag indicators for clone firms or entities being used to commit economic crime, that are relevant for CDD checks:

- Use of Companies House default postcodes and addresses (see below);
- Company has changed its registered office many times;
- The customer's registered office and principal place of business are not at the same location, and the principal place of business does not appear to be used for the business of the customer;
- Name of entity similar to a well-known brand;
- Five letters of a director's name in the company name; and
- Dormant Companies House SIC code.

These red flags should be considered alongside other general red flags around the obfuscation of ownership and control (e.g. no Person of Significant Control, complex/opaque ownership structure, use of nominee directors and shareholders) or red flags such as high-risk jurisdictions.

Use of Companies House Default Address

Companies House has default addresses that it can use where a registered office address is disputed (via the RP07 process – see above). When checking the Company Register for information about a potential or existing client, the use of a CH14 postcode, or PO BOX 4385, 07078853: Companies House Default Address, Cardiff, CF14 8LH, in the company's filing history may be a red flag that the company has used an address fraudulently.

Use of Companies House Data as Part of CDD
Companies House provides a Free Company Data Product, which is a downloadable data snapshot containing basic company data of live companies on the register. The webpage provides links to a series of zip files containing CSV formatted data. Regulated entities may be able to utilise this data to search for: their own postcode, postcodes of their customers, the names of their own business, the names of their customers to identify clone firms.

Some regulated entities may find using the advanced search function on the Companies House website as an easier tool to identify red flags about a potential client at take-on or as part of ongoing monitoring procedures (Advanced company search - Find and update company information - GOV.UK (company-information.service.gov.uk).

FCA Warning List of Unauthorised Firms
Scammers often use cloned firms (i.e. they pretend to be a firm the FCA authorises) to provide an air of legitimacy to their illegal activities. Clone firms often use the name and address of a genuine, authorised firm.

The FCA maintains a Warning List of unauthorised firms and individuals that they are aware of, but that aren't allowed to operate in the UK.

Solicitors Regulation Authority Scam Alerts
Scammers often pretend to be regulated entities to give themselves an air of respectability. The Solicitors Regulation Authority (SRA) maintains a list of Scam Alerts to warn consumers about people who call themselves solicitors but are not.

Anti-fraud Databases and Information Sources.
Regulated entities may be able to register with anti-fraud databases (such as CIFAS) to access information about companies who are suspected of committing fraud.

There are many blogs and social media accounts by investigative journalists who publish information on economic crime.

UK Regulatory Response

The UK government are seeking to address gaps in corporate transparency laws with legislative reforms. The most recent piece of legislation is the Economic Crime and Corporate Transparency Act 2023 (ECCTA), which delivered a suite of wide-ranging reforms to tackle economic crime and improve transparency over corporate entities. ECCTA equipped the Registrar with investigation and enforcement powers, enabling them to check, challenge and reject information filed at Companies House, allowing Companies House to be a 'proactive gatekeeper'.

This alert provides advice and methods available at the time of issue of the alert, but JMLIT and the Fraud Money Laundering Threat Group will consider updating the alert when new powers and/or reporting routes are in use.

Reporting routes for regulated businesses that identify concerns

If a regulated entity identifies concerns that involve virtual squatting, they should consider whether they need to make a report to a relevant authority.

Suspicious Activity Report - If you identify activity which may be indicative of the activity detailed in this report, and there is a proceed of crime, you may wish to make a Suspicious Activity Report (SAR). If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include **XXJMLXX** within the text and the reference **0742-NECC** for this alert within the relevant field on the NCA SAR Portal.

Action Fraud – Action Fraud is the UK's national reporting centre for fraud and cybercrime. They take reports on behalf of the police and every report we receive helps to build a clear picture of fraud and cybercrime, making the UK a more hostile place for criminals to operate in. You can report fraud via the website.

Trading Standards – If you think a business has broken the law or acted unfairly, you can report them to Trading Standards. Trading Standards use the information you give them to investigate unfair trading and illegal business activity, like rogue traders and scams.

FCA – if you believe the virtual squatting is related to a financial product scam, you can report the matter to the FCA. Report a scam | FCA

Insolvency service – The Insolvency Service can conduct a confidential investigation into an active limited company (LTD) or limited liability partnership (LLP), where it has received information suggesting serious corporate abuse. If such abuse is found, it can apply to the court for the company to be wound up. Live company investigation - what we do Complain about a limited company

Data Protection Considerations

Please consider your obligations under the relevant data protection regulations and where necessary remove any related personal data from your systems securely and within a satisfactory timeframe.

Disclaimer