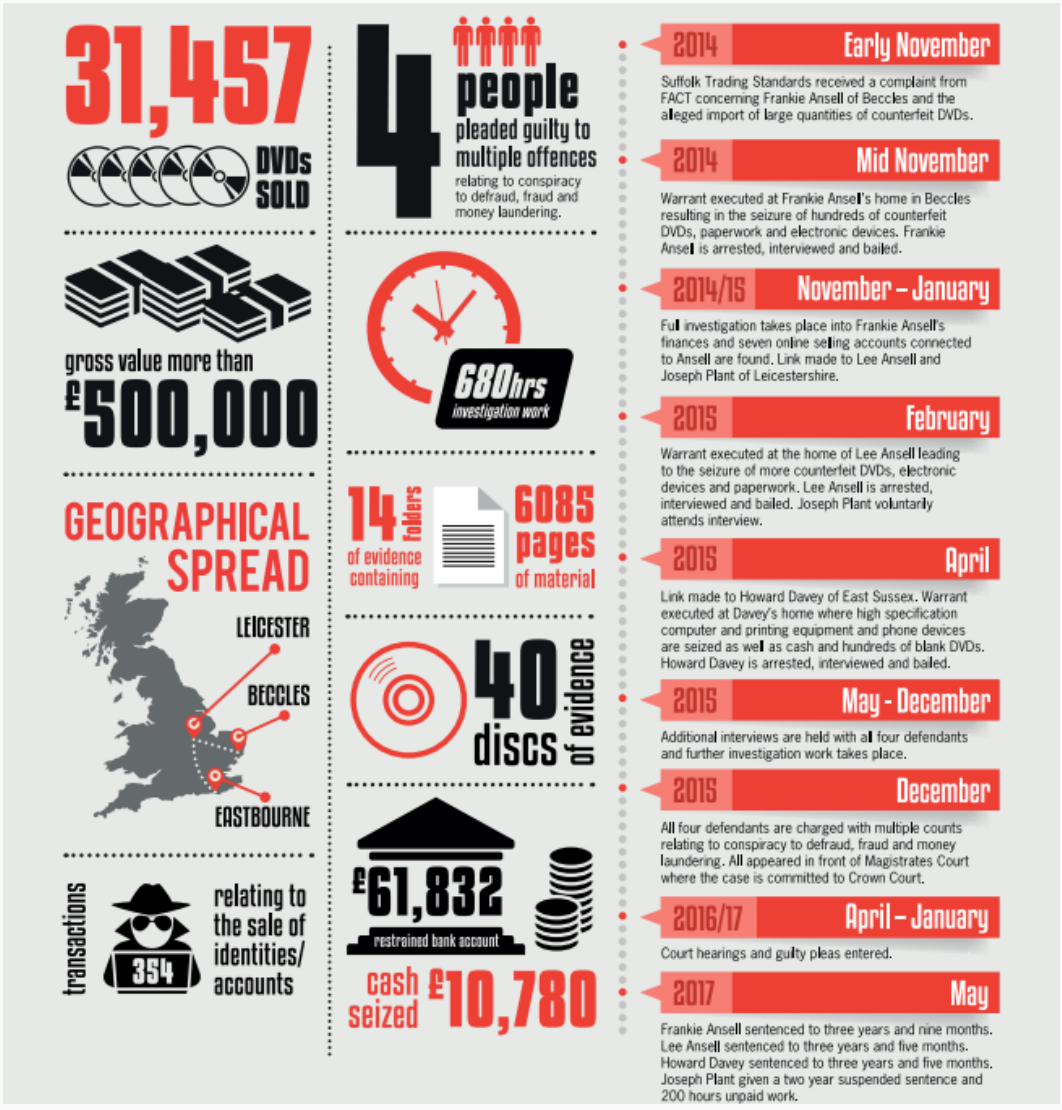
JOIN THE FIGHT
Suffolk Consumer Champion Weekly Bulletin

26/05/2017

This week's top features



Three men jailed for sophisticated fake DVD operation

Three men were jailed for a total of 10 years and seven months for selling fake DVDs following a successful investigation by Suffolk Trading Standards.

Frankie Ansell, of Grove Road, Beccles was jailed for 45 months and his cousin Lee Ansell, of Stonebow Close, Loughborough was jailed for 41 months. Howard Davey, of Esher House, Eastbourne, received a 41 month prison sentence.

Joseph Plant, of Heathcoat Street, Loughborough, received a 16 month sentence, suspended for two years, and was also ordered to undertake 200 hours unpaid of unpaid work.

The four men managed the sophisticated counterfeit DVD business over a two-and-a-half-year period, selling over 31,000 DVDs, worth more than £500,000.

The operation involved the use of fake identities and paperwork, as well as money laundering practices. Suffolk Trading Standards began the investigation when they received a complaint from FACT concerning Frankie Ansell and the sale of counterfeit DVDs. A search of his home in Beccles followed and led to the seizure of £5,670 in cash, 600 counterfeit DVD titles, and electronic devices.

Suffolk Trading Standards then identified other individuals involved. Warrants were executed for Lee Ansell and Joseph Plant in Leicestershire and Howard Davey in Eastbourne.

These resulted in the seizure of a high specification computer, along with laptops, tablets, and mobile phones. Also seized was £5,000 in cash, £1,250 worth of gift cards, two DVD copying towers, a laser printer, as well as hundreds of blank DVDs.

Protect Yourself Against Ransomware

The National Cyber Security Centre is currently working with organisations and partners in the UK affected by the ransomware 'WannaCry'. This page contains guidance for home users or small businesses who want to reduce the likelihood of being held to ransom by WannaCry (or other types of ransomware).

- This guidance will be updated as more information becomes available.
- There is more general advice and guidance on protecting yourself online at CyberAware.

What is WannaCry?

WannaCry is a type of malicious software known as *ransomware*. Ransomware makes your data or systems unusable until the victim makes a payment.

What can I do to protect myself?

There are three main things you should do to protect yourself.

1. Update Windows

WannaCry only affects computers running Microsoft Windows operating systems that don't have the latest security patches installed. If you are using a recent version of Windows (Windows 7, Windows 8, Windows 8.1 or Windows 10) and have automatic updates turned on, you should already be protected automatically against WannaCry.
To update your version of Windows:

- If you are using a currently supported version (Windows 7, Windows 8, Windows 8.1 or Windows 10), run Windows Update and apply any updates.
- If you are using Windows XP, Windows Vista or older versions of Windows, download the WannaCry security update from here and install it.

Note: We strongly recommend that you do not continue to use unsupported operating systems, but instead upgrade to one which receives regular security updates from the vendor.

2. Run antivirus

- Make sure your antivirus product is turned on and up to date. Windows has a built in malware protection tool (Microsoft Defender) which is suitable for this purpose.
- Run a full scan to make sure your computer is currently free of all known malware.

3. Keep a safe backup of your important files

- Regularly create a backup copy of your important files (such as photos, documents, and other files that can't be replaced). If you have backups of files that you can recover, you can't be blackmailed.

- Make sure that this copy is kept separate from your computer. If it's on a USB stick, or a hard drive, or on any type of removable media, do not leave it connected (or anywhere on your network) or it may also be attacked by ransomware.
- You should consider using cloud services to back up your files. Many cloud service providers (for example, email providers) offer an amount of cloud storage space for free.

What to do if you have been infected with ransomware

The National Crime Agency (NCA) encourages anyone who thinks they may have been subject to online fraud to contact Action Fraud at www.actionfraud.police.uk.
If a small business has been a victim of ransomware and are worried about the infection spreading to other parts of your network, these steps may help guide your actions:

- Immediately disconnect you computer, laptop or tablet from network. Turn off your Wi-Fi.
- Safely format or replace your disk drives.
- Whilst you're still disconnected from your network, directly connect this computer to the Internet.
- Install and update the operating system and all other software.
- Install, update, and run antivirus software.
- Reconnect to your network.
- Monitor network traffic and/or run antivirus scans to identify if any infection remains.

Files encrypted by the WannaCry attack have no way of being decrypted by anyone other than the attacker. Don't waste your time or money on services that are promising to do it.

Should I pay the ransom?

The NCA encourages industry and the public not to pay the ransom. If you do:

- There is no guarantee that you will get access to your data.
- Your computer will still be infected unless you complete extensive clean-up activities.
- You will be paying criminal groups.

Learn How to Spot Illegal Tobacco at The Suffolk Show

This year we will be at the Suffolk Show with our Illegal Tobacco trailer and sniffer dogs.

If you are visiting, you can find out about the work we do to stop illegal tobacco being sold in Suffolk, how the sniffer dogs find a hidden concealment of illegal tobacco, as well as how you can spot illegal tobacco and report it.

Come and find us on stand 243 on Flower Show Avenue.

Product Recalls

Fraud and Scam Advice

Consumer Rights


Checkatrade.com
Where reputation matters
Suffolk
County Council
TRADING
STANDARDS
APPROVED