Passing the buck

RECENT CRIME FIGURES SHOW DISTURBING LEVELS OF ONLINE FRAUD. **ZOË BLACKLER** ASKS IF ENOUGH IS BEING DONE TO HELP THE VICTIMS

For their trip to Amsterdam, Anne and Paul Deardon found the perfect apartment on a holiday lettings site. Although they'd used the site before, when they were asked to pay by bank transfer rather than input credit card details, they thought nothing of it. A few weeks later, they saw a photo of their rental in a national newspaper. It was an example of a growing type of online fraud, the holiday-rental scam.

In July, the ***Crime Survey*** for England and Wales included, for the first time, figures for fraud and scams. The results – from a survey of 35,000 households and considered the most accurate picture we have of UK crime patterns – were wildly at odds with the official reporting figures. While the survey estimated a total of 5.77m incidents of fraud and computer misuse between April 2015 and March 2016, only 222,502 were reported to the fraud reporting body, Action Fraud. Which means that just one in every 26 instances of cyber-crime were reported by the public to the police.

Even for the small number of victims who do contact the police, the chance that a report will turn into a criminal investigation is extremely low. The victim's bank may reimburse them, but the likelihood of money being recouped by the police, experts say, is close to negligible. Here, we ask if cyber-crime victims are being failed by the authorities meant to help them.

WHO YOU GONNA CALL?

If you came home to find your car had been stolen, you'd know to call the non-emergency police number, 101. But if you realised your online bank account had been hacked, who would you call? We tried to find the definitive answer and discovered something alarming: there isn't one.

According to official advice, you should call Action Fraud. Set up in 2009, it's meant to be the equivalent of 101 for scam victims. You can report online or via its helpline. Once you've contacted Action Fraud, it sends your details to the National Fraud Intelligence Bureau (NFIB) for review. The NFIB can't investigate cases itself, but if it considers there are 'viable lines of enquiry' it will pass on the case to your local police force, which will decide whether to start an investigation. The process, says Action Fraud, should take no more than 28 working days.

Yet certain types of cyber-crime cases could be reported to Trading Standards. If you've been duped into handing over cash for goods or services that didn't materialise, Trading Standards is charged with investigating. Its remit includes fake online shopping sites, flight and ticket scams, and holiday lettings scams like the one experienced by Anne and Paul.

But the lines of responsibility aren't clear cut, admits Mike Andrews of ***National Trading Standards***' eCrime Team. If you've paid a 'deposit' to someone pretending to let you a flat, would it be a case for Trading Standards or Action Fraud? 'A grey area,' he says.

This confusion prevents some reporting. 'It's hard to put a figure on it,' says Andrews, 'but inevitably there will be some loss because people don't know where to report.' Which is why, he says, increasingly Trading Standards and Action Fraud share cases. You can't make a report directly to Trading Standards, though. You have to do it via Citizens Advice. So perhaps Citizens Advice should be your first stop? Its call handlers would know whether to help you make a report to Trading Standards or advise you to report to Action Fraud. Wouldn't they?

We asked Citizens Advice to explain the advice it gives to scam victims. It declined an interview, but sent a written statement from senior consumer expert Jan Carton. Recognising that Citizens Advice was often the 'first port of call' for scam victims, taking 20,000 calls a year, Carton told us: 'When advisers identify a breach of the law, they pass the case to Trading Standards to investigate.' While the statement said that it supports local bureaux to share insights with police and crime commissioners, it did not mention directing victims to Action Fraud.

Confused? You're not alone.

WHAT YOU'LL LEARN

We've interviewed insider-sources from the fight against fraud. Find out:

- Who to call if you've been scammed
- How police are struggling to keep pace with rising levels of fraud
- Why some scam victims are reimbursed and others lose thousands

SHOCKING DELAYS

When the Deardons realised they'd been scammed, they called the local police station, which referred them to Action Fraud. They were given a crime number and told to expect an update within 28 working days.

Two months passed before Action Fraud wrote to the Deardons to tell them that their case had been passed to the Met Police for investigation. However, the letter was dated a day after the Met wrote to say that there were no viable lines of enquiry and the case had been closed.

In June, Garry Lillburn, a detective inspector from the Met's fraud unit Falcon, speaking at an information security industry conference, bemoaned the current reporting process: 'We in law enforcement are obliged to work with the system the Home Office dictates. Sadly, that system is Action Fraud.'

'If you were to call your local police force, they'll tell you to go to Action Fraud. They're not cyber officers and that's where the confusion comes in.'

Even a delay of a week hampered effective investigation, he said. 'I've seen things come in sometimes four weeks after they're reported, and that's shocking.'

His damning assessment of Action Fraud is supported by Her Majesty's Inspectorate of Constabulary ***(HMIC)***. In December, HMIC published its study into police responses to cyber-crime. One force crime manager told researchers: 'In general, a crime reported to Action Fraud would take at least 30 days before it's allocated to an investigator in force.'

As HMIC notes, a large proportion of the £3.5bn in losses reported to Action Fraud between April 2014 and March 2015 were originally transferred to an account in the UK. But the timeframe in which to freeze those accounts and recover the funds is tiny, HMIC adds. Often that money has gone within 24 hours – transferred by criminals to foreign accounts far beyond the jurisdiction of UK police. This long delay between Action Fraud taking the report and a local officer opening an investigation 'presents a substantial opportunity to the offender,' HMIC said.

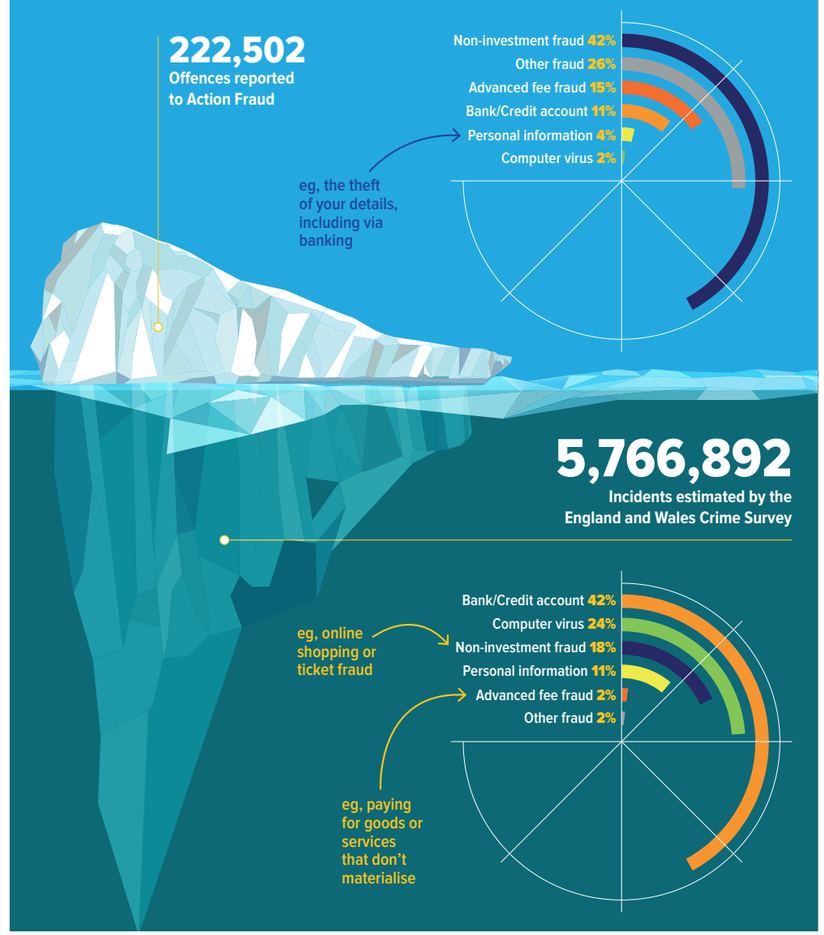
FOLLOW THE MONEY

But it wouldn't be fair to put all the blame for the dismal investigation rates on Action Fraud. In its report, HMIC found that Action Fraud, 'seems to be used by local forces to offload fraud victims and hide its own lack of interest in tackling these crimes'. Victims are referred to Action Fraud, 'even when local officers could have done something quickly to remedy the situation'. While the Deardons' case was moving at a glacial pace through the system, they were also in touch with their bank.

Experts agree that if you have any hope of getting your money back it will be via your bank, but if you've authorised a transfer the bank has no legal responsibility to refund you. Act quickly and there's an outside chance it may just be able to trace and freeze the funds. But don't assume that it will act as >

THE TRUE SCALE OF FRAUD

Just one in 26 fraud incidents is reported to Action Fraud. Estimates from the England and Wales crime survey 2015/16 reveal how much fraud goes unreported.



BEWARE BANK TRANSFERS

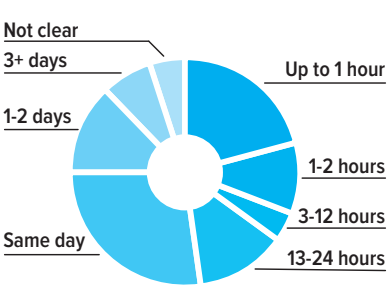
One of the most notable areas of under-reporting of cyber-crime is card fraud. It's not surprising. By law, your bank must refund you if your credit or debit card has been used for a fraudulent payment, as long as you've not been negligent, so victims have little incentive to file a crime report. But your bank has no such duty if you're tricked into making a bank transfer.

As online criminals have become more inventive, some customers have lost tens, or even hundreds of thousands of pounds in this way, with no chance of ever being refunded.

One Which? member told us how fraudsters claiming to be from NatWest convinced her that her account had been compromised and to transfer her £17,500 savings to another account, apparently in her name. Within minutes she realised she'd been tricked, but when she contacted NatWest, she was told her money had gone and was referred to Barclays, the receiving bank. Barclays said the fraudsters had cleared the account and they were unable to trace the funds. Without admitting liability, Barclays offered to refund her the 10p the fraudsters had left behind.

Her story is just one of many that have come to our attention. We think this is a serious gap in consumer protection and will be seeking to raise the issue with government and the regulator.

Slow to act: 25% of sending banks took more than a day to contact the receiving bank after transfer scams



Source: Financial Ombudsman Service

> IF YOU DO GET SCAMMED YOU HAVE TO ACT QUICKLY

swiftly as it should. The ***Financial Ombudsman Service*** reported recently that in some scams involving authorised transfers, the bank was slow to act. Some 34% of payees' banks took more than 12 hours to contact the receiving bank, and 12% took more than three days.

In the Deardon's case, their story took an unusual turn. The fraudsters hadn't cleared out the receiving account, and Anne and Paul got their £1,100 back.

A GROWING CHALLENGE

Criminologist David Kirk, who chaired a recent independent report by the Fraud Advisory Panel, is careful not to be too critical of Action Fraud – it has a good call centre, he says – and the NFIB now has 100 staff. There are plans to improve its website. But the experience for victims, he says, is far from satisfactory. And once a scammer has your money, it's near impossible to get it back. This will only get worse as the number of victims continues to increase. 'It's difficult not to sound hopeless,' Kirk says.

The NFIB's current approach is to look for the organised gangs behind multiple scams, rather than attempt to tackle every individual crime.

But, argues criminologist Michael Levi, the problem of cyber-crime demands a different approach. Levi compares the pressures placed on the police by fraud to those on the NHS. Fraud investigations could suck up limitless resource if we let them. We need a debate on what's possible and to make sure the emphasis is on prevention.

WHAT TO DO

While the situation may seem dire, there are things you can do to protect yourself (see 'Take action', below).

If you do get scammed, you have to act quickly. First stop: your bank. Next, your local police force – you'll probably be referred to Action Fraud, but you may be lucky enough to find a force prepared to take on the responsibility. Finally, accept that you may have to suffer a financial loss, but report the crime anyway.

'The sheer volume of cases means that each individual report can't be investigated,' admits Trading Standards' Mike Andrews. 'We have to pick our fights.'

However, while the system is struggling with the scale of reports it already gets, Andrews would still like to see every crime reported. It might not help an individual victim to get redress, but could still be hugely beneficial to future victims.

For the police, government and society generally to respond appropriately, we need accurate data that reveals the true scale of this pernicious crime.

TAKE ACTION

WHAT TO DO IF YOU GET SCAMMED

If you lose money to online fraudsters, the police are extremely unlikely to catch the perpetrators and recoup your cash. The most effective action you can take is prevention. Never make a bank transfer to someone you don't know. Call to check the details, especially if they came by email – people have lost hefty amounts after their solicitor's or builder's email accounts have been hacked.

Use a credit card online rather than a debit card, as it gives you greater protections. Keep all your computer software up to date, never click on email links from people you don't trust and be suspicious of cold-callers, especially those claiming to be from your bank.

WHERE CAN I GET HELP?

Which? members get unlimited access to the Which? Money Helpline – a team of experts who can answer your financial queries. Give them a call on **01992 822848**.

WHERE CAN I FIND OUT MORE?

IN *WHICH?* AND *WHICH? MONEY*

- ***Why intelligent people fall for fraud***, *W?*, Sep '16, **p44**
- ***Pension sharks***, *W?M*, Sep '16, **p44**
- ***Can you spot an email scam?***, *W?M*, Aug '16, **p18**

ON WHICH.CO.UK

- Sign our scam campaign: **which.co.uk/safeguard**
- Report a scam: **which.co.uk/howtoreport**
- How to get your money back: **which.co.uk/getmoney**

OUTSIDE OF WHICH?

- **Action Fraud:** actionfraud.police.uk
- **Citizens Advice:** citizensadvice.org.uk
- **Get safe online:** getsafeonline.org