July 2015

Financial Ombudsman Service

calling time on telephone fraud

a review of complaints about "vishing" scams

Financial Ombudsman Service insight report

foreword

Over the past year much of the ombudsman service's work has, once again, focused on resolving complaints made about mis-sold payment protection insurance (PPI). Understandably, the scale of the numbers of complaints involved in PPI and other "mass" mis-selling issues means they often draw the most attention when we publish information about the complaints we're receiving.

But we resolve complaints about a wide range of financial products – from payday loans and mortgages to pensions and pet insurance. And the impact on consumers when something's gone wrong can't be measured or understood simply by comparing volumes of complaints.

A particularly challenging area of our work – because of the nature of what's happened and its impact on the people affected – is financial fraud. Some of the most upsetting situations we've been called into have involved voice phishing, or "vishing"' – in particular, "no hang-up" frauds.

These deceptions can be very convincing – with consumers tricked into believing they're protecting their money, when in fact it is being stolen. Among the people who have contacted us, many have been over 75 and have lost significant amounts of money – in some cases their life savings. And, because of the way the fraud is carried out, most people won't get their money back.

> *"This has been a traumatic experience for me. Not only have I lost all my savings, but I am fearful of answering the phone or door."*
>
> consumer

How these frauds happened – and how the fraudsters will be found and dealt with – are for the police and other authorities to investigate. As an ombudsman service, our role is to resolve disputes where a consumer has concerns about their bank's response to the fraud.

In some cases, we find that the bank's response has fallen short. In many others, we find that the bank's actions have been fair and reasonable. But in both sets of circumstances, we think there are lessons to learn – so that consumers can ensure they protect themselves as best they can against fraudsters, and that banks can ensure they treat their customers fairly when they do fall victim to scams.

One of our key strategic objectives is providing insight to encourage fairness in money matters. It's a commitment we take very seriously. By sharing our unique perspective on what goes wrong in financial services, we believe we can help businesses serve their customers better – as well as supporting effective regulation of the financial services sector.

Action being taken by telecoms companies is already reducing the potential for some kinds of vishing fraud we currently see. But scams are constantly evolving – and the themes and findings we highlight in this report should be applicable to other types of fraud. We hope that by sharing our insight we can contribute to the significant efforts others across the industry are already making to keep people's money safe.

Caroline Wayman
chief ombudsman and chief executive

contents

chapter 1	summary
chapter 2	introduction
chapter 3	how scams happen – and their impact
chapter 4	scams and different groups of consumers
chapter 5	how banks try to prevent vishing scams
chapter 6	banks' action once fraud has been detected
chapter 7	security and convenience
chapter 8	how banks handle complaints about scams
chapter 9	the future of the no hang-up scam – and lessons to learn
annex	about the ombudsman

chapter 1 summary

"vishing" and "no hang-up" frauds

- **Vishing** (voice phishing) is the criminal practice of using the phone to defraud, dupe or mislead someone. A particular form of vishing that's caused concern is the **"no hang-up" scam**. Here, fraudsters – usually posing as the police or a bank – persuade consumers that their account is at immediate risk. Fraudsters tell consumers that they need to move or withdraw their money urgently to keep it safe, using a technical trick on the phone line to add to the plausibility of the scam and to gain access to consumers' private personal and financial information.
- The ombudsman service sees different forms of "no hang-up" frauds in the complaints that are referred to us. Most involve **online** money transfers, but some transfers take place **in-branch**. In some cases, consumers are tricked into **giving away their account and PIN details** over the phone. Others give their cards directly to a fraudster – believing them to be a "**courier**" for the bank. Some people have withdrawn money to give to such "couriers".

what we looked at

- Between mid-2012 and the end of 2014, the ombudsman service resolved **185 complaints** involving a no hang-up scam. We conducted a detailed review of each of these complaints, looking at the nature of the fraud carried out, why consumers brought their complaint to us and what lessons could be learned for the future.
- We also spoke to a **wide range of organisations** to help us understand the context for what we were seeing. This is important because generally we won't be party to the circumstances of complaints that businesses have resolved directly with their customers.

the consumers who brought complaints to us

- The 185 complaints involving a no hang-up scam were brought by **173 individual consumers**. Some people had more than one complaint – typically against different banks

relating to the same fraud. Older consumers were disproportionately represented in the complaints we reviewed – with **80% of those affected aged over 55**. Most were over 65 and many were **over 75**.

- We found some geographical patterns in the complaints we reviewed – with consumers particularly concentrated in London (28%), the south east (26%) and the east of England (16%). Men and women were equally likely to have brought a complaint to us about a vishing scam.

the financial impact

- In the complaints we reviewed many consumers had lost substantial sums of money – in many cases tens of thousands of pounds. Altogether, the 185 complaints involved losses of up to **£4.3 million**.
- A fifth of the consumers had lost between **£20,000** and **£49,999** – but one in ten had lost more than that. The largest individual loss we came across was **over £100,000**.
- Banks have a duty to act on their customers' instructions. So if a consumer transfers or withdraws money *themselves* during a scam, they're unlikely to get it back.

why consumers complained

- The *main* reason for consumers complaining to us about their bank's response to a no hang-up scam was a feeling that the bank was responsible for the loss and should have refunded the money (**56%**). This was followed by a belief that the bank could have done more to stop the fraud taking place (**21%**).
- We also looked at *all* reasons for complaining – looking both at the main reason for complaining and at any additional reasons that were apparent in the cases we reviewed. In a third (**34%**) of cases, we found consumers were unhappy with the customer service they had received from their bank in the aftermath of the fraud.
- In the sample we reviewed, the ombudsman service upheld **37%** of the complaints in the consumer's favour. This is broadly in line with the average proportion of complaints about banking that we uphold.

banks' handling of "no hang-up" frauds

- In our review, we saw both good and bad practice by the banks involved. In a third of the cases we looked at, we were able to identify **warnings** that the banks had given their customers about possible vishing fraud. Based on the complaints we've seen over the years, it's clear that the financial services sector has invested considerable effort in this area.
- While there is no duty to do so, most banks believe it is good practice to question or query large or unusual transactions made in-branch, particularly those made by older consumers. But we found a mixed picture and inconsistency when it came to this.
- We found a lot of evidence suggesting that banks had acted quickly when alerted by customers that they had been defrauded. But we saw some cases where the "sending" bank – the one given instructions to transfer money – had taken a long time to contact the "receiving" bank to try to recover the consumer's stolen money.
- Some consumers told us that their bank had given them incorrect information – for example, that they would be likely to get their money back when this turned out not to be the case.

some lessons to learn

- The "no hang-up" loophole that allows this fraud to take place is expected to be closed by telecoms companies later this year. But vishing-type frauds are continually evolving – and our findings are relevant to telephone fraud more generally.
- On the basis of the complaints we reviewed, we're able to highlight some areas where all affected parties could work together more effectively to help prevent fraud.
- The banks have made significant efforts to warn their customers of the risks, including a joint warning through Financial Fraud Action UK. Because of the way frauds change and develop it is likely there will be a continuing need for co-ordinated work of this kind across the industry.
- Consumers have told us they feel it would be helpful if all banks had a consistent approach when it comes to asking about large transactions made in branches.
- Consumers need to be aware of the risk of fraud – and be very careful with their bank security details and personal information. They should also be wary of "cold calls", whoever the caller claims to be – and whatever number comes up on the "caller ID". And people

shouldn't delay in taking action if they think they've been the victim of a scam – by reporting it immediately to their bank and the police.

- For most victims of telephone fraud, the experience has an emotional as well as financial impact. The treatment victims receive after the fraud – from their bank, the ombudsman or other organisations – can make a big difference. That means listening, showing empathy and clearly explaining what's happened, how things stand, and why.

chapter 2 introduction

financial fraud in the UK

Over £570 million of financial fraud was committed in the UK in 2014 – and over the year, online banking fraud increased from £40.9 million to £60.4 million.[1] Action Fraud – the national reporting centre for fraud and internet crime – logged 1,028 instances of consumer phone fraud in 2014.[2]

A growing area of concern has been the increase in fraudsters impersonating banks and police over the telephone – which is commonly referred to as voice phishing, or "vishing". According to Action Fraud, vishing scams accounted for £23.9 million of losses between December 2013 and December 2014 – more than triple the £7 million recorded in the previous year.[3]

The number of bank accounts being opened using a stolen or fictitious identity has also nearly doubled – with over 23,600 cases reported in 2014 compared to 12,500 in 2013.[4]

box 1: the 'no hang-up' trick

A "call party hold" feature is available on some UK landlines. This means that phone calls aren't disconnected for several minutes after one person hangs up – if the other person stays on the line.

Fraudsters have exploited this feature. They call consumers, warning that their current accounts are in immediate danger and urging them to act quickly to safeguard their money.

In the complaints that we see, fraudsters have often encouraged consumers to call the genuine number for their bank or the police to verify that their call is authentic. This can add to the believability of the scam.

But because of the "call party hold feature" the fraudster can stay on the line. By impersonating the bank, they're able to secure personal banking details, or to convince consumers they need to withdraw or transfer money to a different account.

[1] Financial Fraud Action UK, "Scams and computer viruses contribute to fraud increases – calls for national awareness campaign", Press Release, 27 March 2015. The quoted figure comprises fraud on bank cards, online banking, telephone banking and cheques.
[2] Office for National Statistics, *Crime in England and Wales, year ending December 2014*, 23 April 2015, Appendix, table A5.
[3] Action Fraud, "New figures show steep rise in telephone scams", Press Release, 2 December 2014.
[4] Cifas, *Fraudscape: UK fraud trends 2015*.

"no hang-up" frauds

The ombudsman service is called into a wide range of complaints related to disputed transactions and fraud. In the last year we have handled several thousand complaints arising from unauthorised payments or fraud.

We've been particularly concerned about the complaints we've been called into that involve a certain type of vishing fraud – "no hang-up" scams. We first started to see them in mid-2012. They centre on a technical feature of telephone landlines which fraudsters can exploit to trick consumers into believing they're talking to their bank or to the police. Told by fraudsters that their bank account isn't secure, consumers have ended up unwittingly transferring money to fraudsters – or handing over details that enable criminals to access their accounts.

We've seen a number of different forms of this scam, including:

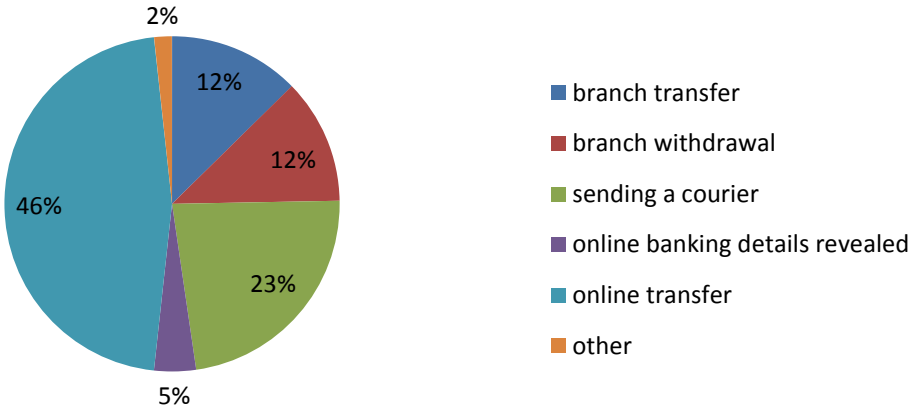
- fraudsters persuading consumers to **transfer funds to a new account**, online or in-branch
- fraudsters persuading consumers to **withdraw money in-branch** to give to a fraudulent "police courier"
- fraudsters deceiving consumers into **revealing their PIN** (typically by punching the number into their telephone keypad) and sending a fraudulent "courier" to collect cards
- fraudsters deceiving consumers into **revealing their online banking details**.

"'Vishing' is a broad term relating to all voice phishing. It seems to have been around forever – but the "no hang-up" trick has significantly altered the wider landscape of telephone scams, including the cost to consumers."

Ray Neighbour, ombudsman

The most common type of no hang-up fraud we've seen involves an online transfer.

figure 1: variations of "no hang-up frauds" in the complaints we reviewed



source: Financial Ombudsman Service. Base: 173 individual consumer complaints.

what we reviewed

Between mid-2012 and the end of 2014, we resolved 185 complaints involving "no hang-up" scams.[5] We carried out a detailed review of these cases. We looked at what action fraudsters had persuaded consumers to take, when incidents were reported, and how banks handled them. We looked at the reasons why people brought their complaint to us – and whether particular groups of consumers were more likely to fall victim to this scam than others.

We know that the numbers of complaints reaching us isn't necessarily a reliable indication of the overall national numbers of this type of scam. This is because we generally won't see complaints that businesses have resolved directly with their customers. As a service, we see only the most entrenched disputes – where businesses and their customers can't agree on a fair outcome to the situation in hand.

box 2: phishing, vishing, smishing...

phishing is when fraudsters send emails to consumers asking them to send personal financial information, such as passwords or bank card details. The email will appear to be from a legitimate sender, including banks

vishing, also known as voice phishing, is the practice of using the telephone to defraud, dupe or mislead individuals. The "no hang-up" scam is one of many types of vishing

smishing is when fraudsters gain personal information through sending text messages

[5] The incidents in the complaints we looked at took place between 1 June 2012 and 15 September 2014 with over half of cases concerning events taking place in 2013. 185 cases were brought by 173 consumers: some consumers brought a complaint against more than one bank. Where needed, we have adjusted the figures in this report to take account of this. For context, the ombudsman service dealt with a total of 9,145 complaints relating to unauthorised or fraudulent transactions over the same period.

Piecing together a bigger picture is also complicated by the fact that information about financial fraud is collected in different ways by different agencies. Definitions of frauds such as "vishing" vary considerably. And some people who fall victim to scams feel too embarrassed or ashamed to report it at all.[6]

But while it's difficult to reach a definitive national statistical picture, there's no doubting the scale of the upset caused by this fraud. Many of the consumers who have come to us have told us of the devastating impact these scams have had on them – financially, emotionally, and physically. Because of the damage wreaked on those who have been deceived by these scams, because many of those affected have been older people, and because there could be wider lessons to learn, we felt it was important to share our insight.

why people had complained to the ombudsman

For each complaint we reviewed, we identified the *main* reason for the consumer's complaint as well as any *additional* reasons that were apparent from the evidence we saw.

The results show that the main reason for complaining was a feeling that the bank was responsible for the loss – and should have refunded the money (56%). Consumers also felt that their bank could have done more to stop the fraud taking place (21%).

These two main reasons for complaint were key overall themes. But consumers' unhappiness at the level of customer service they had received (featuring in 34% of complaints to some degree), and unhappiness that their bank hadn't done enough to recover the lost money (20%), were also prominent reasons for complaining.

[6] Research by the University of Exeter on behalf of the Office of Fair Trading in 2009 found that not reporting a scam might be a way for the victim to avoid "further thinking about being defrauded", which had already caused them distress and anger. See: Office of Fair Trading, *The psychology of scams: provoking and committing errors of judgment*, May 2009, p. 23.

table 1: reasons for complaining to the ombudsman about a "no hang-up" fraud

	main reason for complaint	*all reasons for complaint*
Bank responsible for loss and should provide refund	56% (103)	73% (135)
Bank could have done more to stop the fraud taking place	21% (39)	45% (83)
Bank could have done more to recover the lost funds	7% (13)	20% (37)
Consumer unhappy with customer service received	5% (10)	34% (63)
Consumer unhappy with bank's speed of response	5% (9)	12% (22)
Bank could have done more to warn consumers	4% (7)	17% (31)
Consumer unhappy with operating hours of bank or its fraud team	1% (2)	4% (8)
Other	1% (2)	6% (11)

source: Financial Ombudsman Service. Base: 185 complaints, against both "sending" and "receiving"' banks. The number of complaints is given in brackets. The "all reasons for complaint" column includes both main reasons for complaint and any additional reasons. Percentage for "all reasons for complaint"' exceeds 100 as some complaints could feature a range of reasons.

our insight in perspective

"Cases wouldn't come to us if they weren't finely balanced. We have to make hard decisions – that's our job."

Colin Brown, ombudsman

We recognise that we are just one of the services which hears from people who've fallen victim to vishing scams. To help us better understand what we were seeing, we spoke to a number of other organisations. These ranged from consumer organisations and charities including Citizens Advice and Age UK, enforcement agencies such as the police, as well as individual financial businesses and industry bodies such as Financial Fraud Action UK.

We're extremely grateful to everyone who contributed their time and perspectives, which have informed and shaped this report. We hope that our own insight will complement what others have found, highlight good industry practice and areas where things could be improved, and help consumers make themselves less vulnerable to these upsetting frauds.

box 3: working with the Financial Conduct Authority (FCA)

The FCA is the financial conduct regulator, with a strategic objective to ensure that the relevant markets work well. It also has an operational objective to secure an appropriate degree of protection for consumers.

The ombudsman service is run independently from the FCA. We have a distinct and separate role – to resolve complaints quickly and informally, and on the basis of what's fair and reasonable in each individual case.

There are procedures in place for making sure we and the FCA work together effectively. We send the FCA details about the number and types of complaints we handle – and also flag any concerns we have that might require regulatory action. We also meet regularly to share insight on issues that might lead to large numbers of complaints.

Reducing financial crime falls within the FCA's statutory objective to protect and enhance the integrity of the UK financial system and also impacts on its consumer protection objectives. Its "Handbook" of rules and guidance states that firms should have robust systems and controls in place to prevent financial crime and money laundering from taking place.

The FCA takes action against fraudsters involved in certain scams – often those involving investments or financial products. The FCA recognises the significant impact vishing can have on the victims and has taken steps* to make consumers aware of this and other types of fraud.

We have shared the findings of our research with the FCA. We also want to share what we've seen more widely to raise consumer awareness of "no hang-up" scams and encourage conversations about the lessons that can be learned from the complaints that reach us.

* See, for example, the FCA website: www.fca.org.uk/consumers/scams/banking-scams/banking-and-online-accounts; and: scamsmart.fca.org.uk/page/protect-yourself-from-vishing

resolving complaints involving "no hang-up" scams

It is not the ombudsman's role to investigate financial crime. What we can do is look closely at the actions of the financial business (in vishing cases this is usually banks) and their customers – to see if anyone could have done anything that might have stopped the theft from happening.

We consider all the complaints we receive on their own individual facts and circumstances – but our approach takes into account relevant regulations (see box 4). Unfortunately it means that where the consumer has been tricked by fraudsters into making a payment or transfer of funds *themselves*, they are unlikely to be able to get their money back.

But we will also consider a number of other things to assess whether a bank treated their customer fairly. This could include, where relevant, whether the bank made reasonable efforts to help the customer get their money back from the receiving bank, and whether branch staff queried "unusual" transactions. We might also look at the bank's previous warnings to their customers about scam activities if relevant to the case.

Of the 185 complaints we reviewed for this report, we found in favour of the consumer in 37% of cases and in favour of the business in 53% of cases. The remaining 10% of complaints resulted in "a small change in outcome". In practice, this meant that the consumer received *some* compensation in recognition of shortfalls in customer service – but didn't get the substantive outcome they were hoping for.

box 4: regulatory overview

There is a long-established principle that banks are generally obliged to carry out their customers' instructions. The *Payment Services Regulations 2009* say that where a payment is made in line with the payer's instructions it is deemed to have been *correctly made*. That's the case even if the payer has been tricked by a third party into giving those instructions.

Where payment instructions are given by someone *other than* the consumer – for example, where someone else has managed to get access to the account – banks have no valid authority to make the payment. But the consumer might still be liable if they haven't taken proper care of their security information.

Most banks and building societies also include specific details about how they handle unauthorised transactions in their current account terms and conditions – which we may look at as part of deciding a complaint. An example of these terms and conditions might be:

> *"If you tell us that a payment was not authorised by you, we will immediately refund your account with the amount of the unauthorised payment plus any fees and interest we may have charged in connection with the unauthorised payment.*
>
> *We will not refund you if you are responsible for transactions from your account and any fees or interest incurred as a result of those transactions. This is if you authorised the transaction yourself; if someone else used your card, passbook or PIN; or you deliberately, or with gross negligence, disclosed your PIN or security details to someone else."*

chapter 3 how scams happen – and their impact

convincing scams

Looking at the 185 complaints in our review, it's clear that the no hang-up scam relies on a well-executed deception. Consumers who contacted us often emphasised how careful they had always been to protect their money. Many had been suspicious to begin with – and had made a number of phone calls in an attempt to verify the identity of the person they were speaking to.

But unaware of the technical trick that allowed the fraudsters to impersonate their bank or the police, consumers ended up believing that the warnings they were receiving were genuine. And once convinced, they were understandably keen to ensure that transactions or card collections went ahead – to safeguard the money they thought was under threat.

ombudsman case study: "courier" collects cards while consumer is still on the phone

Mr H took a call from someone who said they were from the police. He was told that his debit cards had been compromised. Mr H was convinced by the scam and called his bank's number to check what the "police officer" had said was true.

Mr H didn't realise at the time that the fraudster was still on the line and this was a con to get him to disclose personal security information. He was asked to key his PIN into the phone for verification. And while he was still on the phone to the person he thought worked for his bank, a "courier" arrived to take his bank cards away.

Mr H soon started to feel that something was not right – and contacted his real bank the following day. They confirmed that a significant sum had been removed from his savings account and more money had been withdrawn at cash machines. The bank said they couldn't refund the money because Mr H had been negligent in giving away confidential information.

"I always hide my PIN number when keying it in at the cash machine. But I had no idea I could be duped by punching it into my telephone keypad. I genuinely thought I was speaking to a member of bank staff."

consumer

When the complaint came to us we weren't convinced that Mr H's actions were negligent – as he had believed he was taking necessary steps to secure his accounts. We decided that: "*there was no opportunity for Mr H to reflect on what was happening. He was following directions from people he thought were acting to protect his accounts.*" We upheld Mr H's complaint and the bank refunded his loss in full.

In some cases we saw consumers repeatedly authorising the same transaction to ensure it went ahead, so fearful were they of the potential losses through fraud. Unfortunately this sometimes meant they overcame the security checks put in place by their bank.

ombudsman case study: consumer passes bank security checks

Mr L received a call telling him his current account had been "compromised". He spoke to someone he thought worked for his bank, who instructed him to transfer his money to a new, "safe" account.

"I regard myself as someone who is careful about money and security. I always burn any disused private papers and cover my PIN at card machines.
But on this occasion, I was totally taken in and conned."

consumer

Mr L transferred over £20,000, a process which involved entering a genuine passcode he received in a text message. Shortly after making the transaction, he received a genuine automated phone message from his bank asking if he'd made the transaction, to which he immediately responded that he had.

A few days later Mr L realised he'd been scammed. He complained that his bank could have done more to stop the fraud taking place and should refund the money he'd lost.

We appreciated that this was a particularly distressing situation for Mr L. But on balance, after looking at the details of the case, we felt the bank had taken reasonable steps to confirm that Mr L wanted to make the payment. It had also been a number of days before Mr L realised and reported the scam to his bank. For these reasons we explained to Mr L that we didn't feel the bank could have done anything more and wasn't to blame.

Many consumers reported that the fraudsters had told them that bank staff were colluding in the fraud and couldn't be trusted. In fact, this was part of the manipulation – to ensure that consumers didn't raise the alarm part-way through the fraud. In one case we dealt with, a very elderly consumer had been told by fraudsters not to trust staff in her local branch – and that if they asked about the purpose of her cash withdrawal, which was for many thousands of pounds, she should say it was for home improvements.

The following case study also highlights how fraudsters can use a consumer's trust of people in positions of authority to pull them into the deception.

ombudsman case study: consumer told he was helping fraud squad

Mr O, who was over 80, got a call from a "detective sergeant" in the "police fraud squad". Mr O was told that the police had arrested a man in the local bank branch, but that the police needed further evidence of illegal practice and counterfeit notes being used in the bank. Mr O was told that if he followed the instructions he'd be helping to bring criminals to justice.

Not realising that this was an elaborate hoax, Mr O visited his bank branch, withdrew a significant sum of money and handed it to the fraudsters. During the transaction the genuine bank staff questioned Mr O about his withdrawal – and handed him a leaflet about different types of fraud. But Mr O was insistent and continued with the transaction.

When the complaint reached us we carefully considered what had happened. We felt the bank had done its best to alert Mr O to the risks of fraud. We felt that Mr O had been so taken in by the fraudsters that unfortunately it would have been impossible for the bank to stop him withdrawing the money.

What happened to Mr O illustrates the convincing and effective nature of the deception involved in these types of scam. It also gives an insight into consumers' thought processes and state of mind. Many people told us that having been told that their accounts were at risk they felt panicked, stressed and frightened. They believed they had to take urgent action to safeguard their money.

In the complaints we reviewed we saw cases where fraudsters had kept consumers on the phone for a prolonged period of time – increasing their anxiety and providing further opportunity for manipulation. Believing that they were talking to the police or to their own bank, and alarmed at the prospect of losing their money, few people challenged advice from those they believed were in positions of authority. The nature of the threat, its urgency, and the technical "no hang-up" trick all combined to overcome consumers' security concerns.

> *"The process of being questioned and given instructions by the fraudsters took place over a considerable length of time and I was finally allowed to go to bed, being assured that the information I had given was helping to catch those who were attempting to steal funds."*
>
> **consumer**

the impact of scams

Where consumers have come to trust fraudsters – and to follow their instructions – the results can be devastating. The majority of "no hang-up" cases that come to us are from people who've lost substantial sums of money – often tens of thousands of pounds.

> *"These are life-changing losses."*
>
> **Colin Brown,** ombudsman

Altogether, the complaints we reviewed represented collective losses of £4.3 million.[7] A fifth of consumers had individually lost between £20,000 and £49,999 – and a further 11% had lost even more than that. The largest individual loss in the cases we looked at was over £100,000. These are life-changing sums of money. Some people lost the money they had saved over many years for their retirement. Others lost funds they were relying on for essential purchases. Some had lost their entire life savings.

[7] This figure represents the cumulative total of all the losses reported by the consumers in the sample of complaints we reviewed in this research. Some consumers, of course, will have got a proportion or all of the stolen money back. The figure therefore covers losses to both consumers and banks.

table 2: money lost by consumers in no hang-up complaints

amount of money lost	percentage (number of consumers)
£1-£999	16% (28)
£1000-£1,999	8% (13)
£2,000 to £4,999	7% (12)
£5,000 to £9,999	16% (28)
£10,000 to £14,999	14% (25)
£15,000 to £19,999	8% (13)
£20,000 to £49,999	20% (35)
£50,000 to £74,999	6% (11)
£75,000 to £99,999	3% (6)
£100k+	1% (2)

source: Financial Ombudsman Service. Base: 173 individual consumer complaints.

ombudsman case study: single mum duped out of savings

Ms W was called by someone who said they worked at Visa. She was told that her account had been "compromised" and that she must phone her bank immediately using the number on the back of her card.

Fearing for the safety of her savings – which were many thousands of pounds – Ms W went on to make an online bank transfer to a "safe" account under the instruction of the fraudster. By the time she realised that she had been scammed there was no money left in the recipient account.

Ms W, a single mum, had been saving for essential repairs to her home. Not only were these repairs impossible following the fraud, she was also left in financial difficulty.

The bank offered Ms W £100 for the distress it had caused by suggesting, at an early stage, that she might get her money back. But we explained to Ms W that because she had made the online transfer herself, the bank could not have known the transaction was fraudulent – and we didn't feel the bank was to blame.

The distressing impact of these no hang-up frauds isn't only down to the size of the sums of money involved. It is often made worse because, due to the way the fraud is carried out, it may be extremely difficult (or impossible) for consumers to get the money back.

"The whole scenario has caused my wife and me a lot of sleepless nights and further stress when trying to access our funds from the bank since this happened."

consumer

In nearly three quarters (74%) of the cases we looked at during our review, the consumer hadn't got any money back after the fraud had taken place. Of those cases where banks *were* able to recover some of the money stolen by fraudsters, 47% of consumers received less than one pound for every ten pounds of the money they'd lost.

In these circumstances, particularly where large sums of money are involved, it isn't surprising that these scams can have serious and lasting effects. The accounts we've heard show that some people experience financial hardship as a result of being scammed. And aside from the obvious financial impact, a number of the consumers whose complaints we reviewed described the anxiety and upset they had experienced after being defrauded. Many mentioned the toll on their physical and emotional health.

"The incident has had a profound effect on my mother. She is shaky, no longer answers the phone unless she knows who is calling, blames herself for losing such a huge sum of money and tries not to spend any money on herself. She ended up in tears after reading and signing her account of what happened."

consumer's relative

"It is difficult to describe the worry and anguish that my family and I are going through at this time. I retired last year and the funds taken were to support my wife and I in retirement. I cannot afford to lose this money and just want it returned so we can get on with our life."

consumer

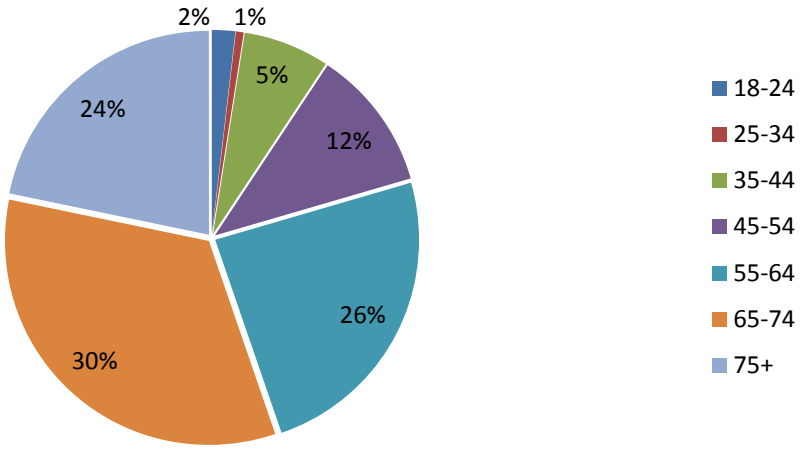
chapter 4: scams and different groups of consumers

older consumers and scams

We found that no hang-up scams affected people of all ages – our sample included consumers aged between 20 and 87. But older consumers were disproportionately represented. We found 80% of the consumers in our sample were aged over 55, more than half were over 65, and a fifth were over 75. There were many in their eighties. Some of the consumers whose complaints we handled said they felt particularly vulnerable because they lived alone, had a serious illness, or had a disability.

> *"A number of factors contributed to my vulnerable state – a bereavement, a major operation and the fact that there had been fraudulent activity on my account two months previously."*
>
> **consumer**

figure 2: no hang-up cases by age group



source: Financial Ombudsman Service. Base: 148 consumers, where the age of the consumer was known.

Because of the stage where we generally get involved in complaints – and the fact that not every complaint reaches us – we can't say for sure, based on our sample, that older people are more likely to fall victim to these scams. But wider research on other types of fraud suggests that people aged over 55 might be more likely to be targets – and so become victims of – certain scams.

> *"Older people may be especially at risk due to social isolation, cognitive impairment or bereavement."*
>
> **Age UK,** April 2015

For example, Age UK recently found that older people are especially at risk of "account takeover", where fraudsters trick people into giving them PIN, account and card details.[8] And from the wider conversations we've had with other organisations, we think our finding that older consumers were more likely to be affected by vishing scams is in line with the bigger picture. This could reflect the fact that older people might be more likely to be at home to receive a potential fraudulent call to their landline, or to have greater resources than younger people – making them a more attractive target.

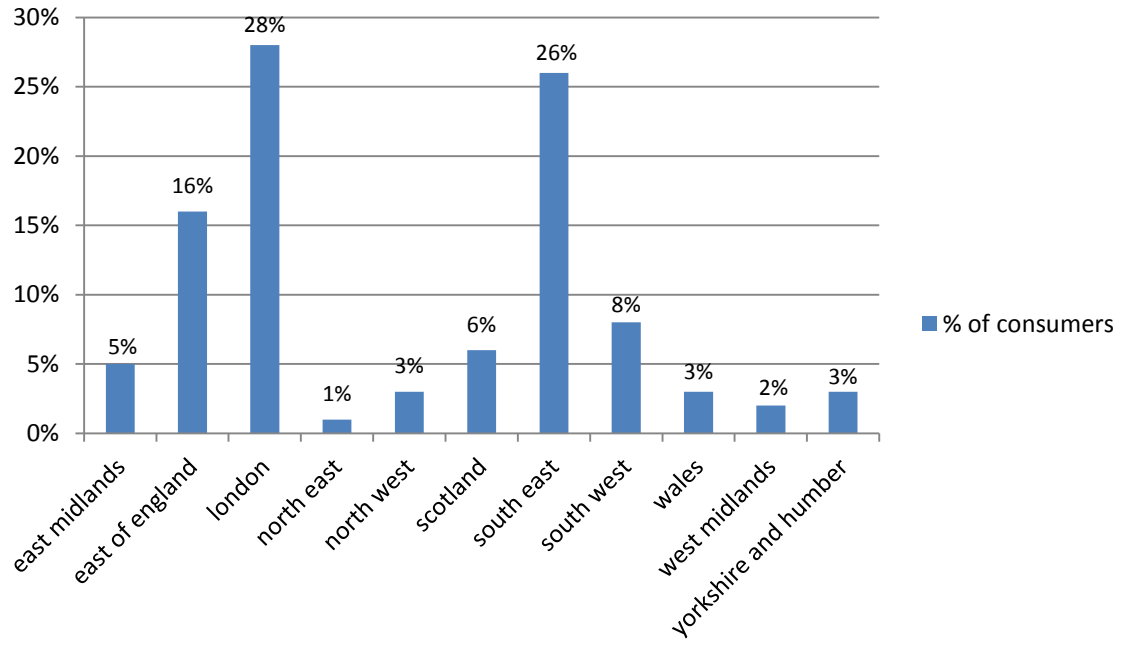
regional patterns and gender

Some media coverage of no hang-up scams has suggested that women are more likely to be targeted than men.[9] But in our own research, we found an equal split between the genders in the complaints we reviewed. We didn't find evidence that gender played a role in either the likelihood of suffering fraud, or the amount of money stolen.

We did see some geographical patterns in the complaints we saw. While our sample included scams across England, Wales and Scotland,[10] there was a noticeable concentration of cases in London, the south east and the east of England.

[8] Age UK, *Only the tip of the iceberg: Fraud against older people. Evidence review*, April 2015, p. 17.
[9] For example, "Will you be the next victim of this oh-so plausible con?", *Daily Mail*, 6 December 2014.
[10] 54% of the consumers involved in our sample of complaints were based in London or the south east of England, and 70% were in London, the south east and the east of England. Although there were no complaints relating to no hang-up scam phone calls from consumers based in Northern Ireland in our sample, we do deal with other related types of complaints from consumers in Northern Ireland. In the period we looked at for this report, consumers from Northern Ireland represented 1.3% of all the complaints related to disputed transactions we dealt with.

figure 3: regional distribution of consumers bringing no hang-up complaints



source: Financial Ombudsman Service. Base: 173 individual consumer complaints.

targeting

In the cases we've seen, many of the consumers believed they had been specifically targeted by fraudsters. Some people suspected that their security details had been stolen. Others believed the fraud had been an "inside job" perpetrated by bank staff.

> *"I believe that the accounts were targeted from information not obtained from me or my computer. I believe the criminals were aware of the large amount of money held in my account and that they were aware of my age, which made me more vulnerable."*
>
> **consumer**

From the cases we reviewed, there was little evidence that allowed us to test whether people had been targeted in this way. But we know that fraudsters can be highly skilled in getting the information they need. This is sometimes referred to as "social engineering".[11] And other organisations involved in tackling vishing have said it's possible that victims may not have been contacted entirely randomly: it's widely known that

[11] "A type of confidence trick, social engineering is the use of deceit to manipulate or trick victims into certain actions. [It] exploits human nature and plays on victims' emotions such as protecting themselves, their family and finances, gaining something of advantage or willingness to please others." Source: City of London Police, *Over £21 million lost to social engineering scams since the beginning of the year*, press release, 25 June 2014.

criminal fraudsters regularly sell on the details of consumers who they think may be susceptible to scams.

"The consumer is giving away information all the time during the fraudulent call. It may be hard for them to decipher or remember what they told the criminal."

Michael Ingram, senior ombudsman

fraudsters exploiting banking inexperience

Some of the consumers that came to us with no hang-up complaints had limited experience of online or telephone banking – making it harder for them to tell whether the instructions they had received were authentic. We found that fraudsters had also incorporated some of the security measures used by banks – such as sending text messages asking customers to confirm that transactions are authorised – into the narrative of the scam.

For example, one consumer told us she had never used online banking before. The fraudster talked her through setting this up on her bank's real system. When she then received a genuine text message from her bank to authorise the payment, she felt reassured she was acting on the bank's instruction.

ombudsman case study: consumer unaware of purpose of "passcode" text message

Mr R was called by someone who said they worked for a centralised bank fraud team. He was told that "suspect activity" had been detected on his accounts and he was advised to call his bank. Mr R did this immediately using the number on the back of his bank card – not realising it was an elaborate scam. He gave security information to the fraudsters believing they worked for the bank's fraud department.

Mr R then received a genuine text message from his bank. The fraudster asked for the code – and said this would cancel a fraudulent transaction. But Mr R hadn't used online banking or passcodes before – and didn't realise that he was in fact authorising a transaction for many thousands of pounds from his account to the account of the fraudster.

When it came to light that Mr R had been defrauded, his bank refused to refund the money, saying Mr R had shared his personal banking details and validated the transfer. But the ombudsman disagreed – because although Mr R had given the passcode to the fraudster, it was the fraudster who typed it in and confirmed the transaction. Mr R had no previous experience of passcodes, and so believed what the fraudster told him about the purpose of the text message.

We upheld Mr R's complaint and he received a refund from the bank.

chapter 5 how banks try to prevent vishing scams

Fraud experts have suggested that one reason for the growth in vishing scams is that increased security around online banking has pushed criminals to look for new ways to defraud people:

> *"Fraudsters adapt their methods – as one becomes more difficult a number of other avenues open up. The increased difficulty in gaining access to existing accounts has occurred at the same time that identity frauds are increasing. Additionally, their attention has been turning to convincing their victims to just give them the money directly. This kind of fraud is often called 'vishing'."*
>
> **Cifas**
> ***Fraudscape: UK fraud trends 2015*, p. 9**

warning consumers

Banks don't have to issue warnings about fraud to their customers. But in a third of the vishing complaints we looked we were able to identify warnings that banks had provided to consumers.[12] These were most likely to be given on banks' websites, but warnings had also been given by post, email or in bank branches. The emphasis on warning consumers of the dangers of vishing and similar frauds was also confirmed in the conversations we had with individual banks as part of our research. Most banks have issued warnings as part of ongoing communications with their customers – for example on login pages for online banking services. But it seems that no two banks do things in the same way.

[12] This is not to suggest warnings were only provided in a third of instances, rather that evidence that such warnings had been given was visible on the face of a third of the complaint files we reviewed in during our research.

ombudsman case study: complaint to ombudsman prompts bank to warn customers

In November 2012 Mrs Q received a phone call telling her that her current account was at risk. She rang what she thought was her bank and was asked to transfer her funds to a new, "safe" account. Mrs Q realised that she had been the victim of a scam the next day – and got in touch with her genuine bank. But by that time the fraudster had withdrawn all the money.

When Mrs Q's complaint came to the ombudsman service, the bank told us that her experience had prompted them to issue warnings to all their customers about this type of fraud.

effectiveness of warnings

In the complaints we looked at there was often a difference of opinion between banks and consumers about whether warnings had been given and whether those warnings had been read or seen. There was also disagreement about whether the warnings were precise enough for consumers to understand the nature of the particular scam – with some consumers complaining that their bank's warnings weren't effective enough to make people think twice in the "heat of the moment".

"The reason the bank gave for not compensating me was that I had not complied with a guidance note under the heading of 'suspicious calls' which is three clicks into a part of its website which you would not normally visit..."

consumer

In one of the complaints we reviewed the bank argued that it had issued numerous warnings and so the consumer should have been aware of the scam. But our adjudicator found the warnings weren't appropriate for this consumer because she didn't use telephone or online banking:

"As you note, Mrs S didn't access telephone banking at any time since warnings have been in place. She also didn't have internet banking facilities. So she wouldn't have been exposed to repeated warnings about this scam.

"You also confirm that she would have received her statement in July which included a warning about the scam. I appreciate that the bank has made

"The bank has done nothing to warn its customers of this type of fraud, or make their cashiers aware of the warning signs."

consumer

efforts to inform their customers about this scam. But I don't agree that by failing to read this small warning, Mrs S was negligent."

missed opportunities

Many of the cases that we've seen involve people who've made online transfers – which are sometimes verified by text or automated phone call. Some consumers have felt that the unusual or large nature of a particular transaction should have triggered a response from their bank. But the scale of internet and mobile banking – accounting for over £6 billion worth of payments a week[13] – makes that inherently challenging and potentially very costly. The automated checking that many banks use gives them assurance that they're fulfilling their obligation to act on their customer's instructions. And the sample of complaints we examined contained examples of banks proactively attempting to stop online payments, as the case study below shows.

ombudsman case study: bank warns consumer while the fraud is taking place

Mr N received a call from someone who said they were from his bank. He was told that security on his account had been compromised and that he would need to move his money to a new "safe" account set up for him at another bank.

Mr N carried out two online transfers, but the second payment triggered the bank's security system. The bank called Mr N to ask him to authorise the payment over the phone. During the phone call with the genuine bank, a member of staff read Mr N a warning about telephone fraudsters pretending to be from the bank and asking customers to transfer money to other accounts. The bank also said that no refund would be made if the transfer was found to be fraudulent.

Unfortunately Mr N was so convinced by the fraudster that he went ahead with the transfer. When it later emerged that he had been scammed, Mr N came to the ombudsman. We considered all the circumstances of the case. On balance, we felt the bank had given clear warnings to Mr N giving him the chance to reconsider his actions. We explained that Mr N had been the victim of a cruel scam, but that the bank was not to blame.

[13] British Banking Association, *The Way We Bank Now*, July 2015, p. 9.

Where withdrawals or transfers are made in a branch or over the phone, there may be greater opportunities for banks to take action to prevent the fraud from taking place. As this scam has become more widespread, branch staff are increasingly aware of the possibility of people making large transfers or withdrawals while they're unknowingly part of a scam. Some of the banks we spoke to said they were training staff on this issue.

ombudsman case study: bank doesn't ask enough questions

Mrs C, in her late sixties, took a phone call from someone she believed to be working for her bank – but who was actually a fraudster. He told Mrs C that she needed to transfer funds to a new "safe" account to protect them from fraud.

Mrs C visited her local bank branch and transferred more than £20,000. The cashier asked if she was "planning to do anything nice with the money?" Later the same day, Mrs C realised she had been the victim of a scam. By this point, the fraudster had taken all the money.

The bank said they wouldn't refund Mrs C's losses because they were carrying out her instructions. When the ombudsman service looked into Mrs C's complaint, we found that another customer had fallen victim to the same scam in the same branch just a few days earlier – putting branch staff on notice of this type of fraud.

We felt the bank should have done more to check that the reasons for Mrs C's transfer were genuine – and could have done more to prevent her losing her money. We told the bank to refund Mrs C in full.

In our research, we looked for evidence in the complaints that had come to us that consumers had been questioned about unusual activity, whether bank staff had had any reason to be suspicious, and whether the bank did anything to make the consumer aware of these types of scam. Most banks recognise it is good practice to query large transactions in-branch, although there is no duty on them to do so. In half of the cases that came to us involving the withdrawal or transfer of money in a bank branch, there were indications that the consumer had been asked

detailed questions about the reasons for the transfer they wanted to make.[14] Some consumers had been questioned extensively, as illustrated by the following case study.

ombudsman case study: bank staff try to stop consumer transferring money from her Isa

Mrs E received a call from "the police" informing her there was potential fraud on her accounts. She was advised to phone her bank immediately – which she did. Her "bank" confirmed the story and said she must transfer her money. Although Mrs E didn't realise it at the time, this was a scam where criminals had used the no hang-up trick.

Mrs E visited her local branch and tried to transfer a significant amount of money from five Isa accounts. Branch staff were suspicious and refused to carry out Mrs E's request. Mrs E visited a second branch to try to make the transfers. Staff in this branch told Mrs E that it would be a bad idea to close her Isas, as she'd lose the tax break and some of the fixed-rate bonds were close to maturity. But Mrs E was insistent and so the bank carried out her request.

In the following days, when Mrs E realised she'd been a victim of fraud she reported it to her bank – but it refused to refund her lost money. A small portion of the money was recovered from the receiving bank. Mrs E brought a complaint against her bank to the ombudsman. We looked at the actions of branch staff and felt that they had repeatedly tried to get Mrs E to think through her actions. Despite this, Mrs E had been particularly insistent that the transfers go ahead. We had to explain to Mrs E that on balance we did not feel that the bank was to blame for the loss.

[14] That is to say, there was evidence in the complaint files we reviewed of detailed questions having been asked of consumers by branch staff. Clearly, such questioning might have taken place but simply not have been captured in the correspondence relating to the complaint. This may therefore be an underestimate.

chapter 6 banks' action once fraud has been detected

raising the alarm

Despite the convincing nature of the no hang-up deception, many consumers realised relatively quickly that they'd been duped and reported the fraud to their bank. We saw some cases where people didn't realise what had happened until their bank contacted them to explain – but most reacted much more quickly.

In those cases where we were able to tell what had happened, a fifth of consumers (20%) had raised the alarm with their bank within two hours of the fraud happening. Overall, three quarters (75%) of the consumers in the complaints we reviewed had contacted their bank about the fraud within 24 hours.

ombudsman case study – consumer becomes suspicious during scam

Mr and Mrs Y received a phone call from "the police" telling them that their bank cards had been used fraudulently. They put the phone down and called their bank from the number on the back of their debit cards. They were told that a "PIN block" was needed to stop the cards being used, and keyed their PIN numbers into the telephone keypad. They were then told their cards needed to be collected by a courier. Unbeknown to the couple, this was a scam. Mr Y did hand over the cards but he was suspicious and followed the "courier" in his car.

At this point both Mr and Mrs Y realised this was a scam. Mr and Mrs Y called the police immediately, and then contacted their genuine bank to block the cards. However, the fraudster had already been able to withdraw £1,000 from a cash machine. The bank said Mr Y had been negligent in disclosing his PIN. But after the complaint came to us, the bank agreed to offer a full refund.

"The Payment Services Regulations say that banks should take reasonable steps to recover money after a mistake. But there is no mistake here. The consumer did order the transaction. That said, under good practice we would expect to see that the bank had taken reasonable steps to help their customer and recover the lost money."

Michael Ingram, senior ombudsman

If fraudsters have accessed cash through a cash machine, or collected money once the consumer has withdrawn cash, there's no opportunity for the bank to retrieve the funds. But there may be an opportunity for a bank to take positive action if a consumer has transferred money to a fraudster's accounts using telephone or online banking.

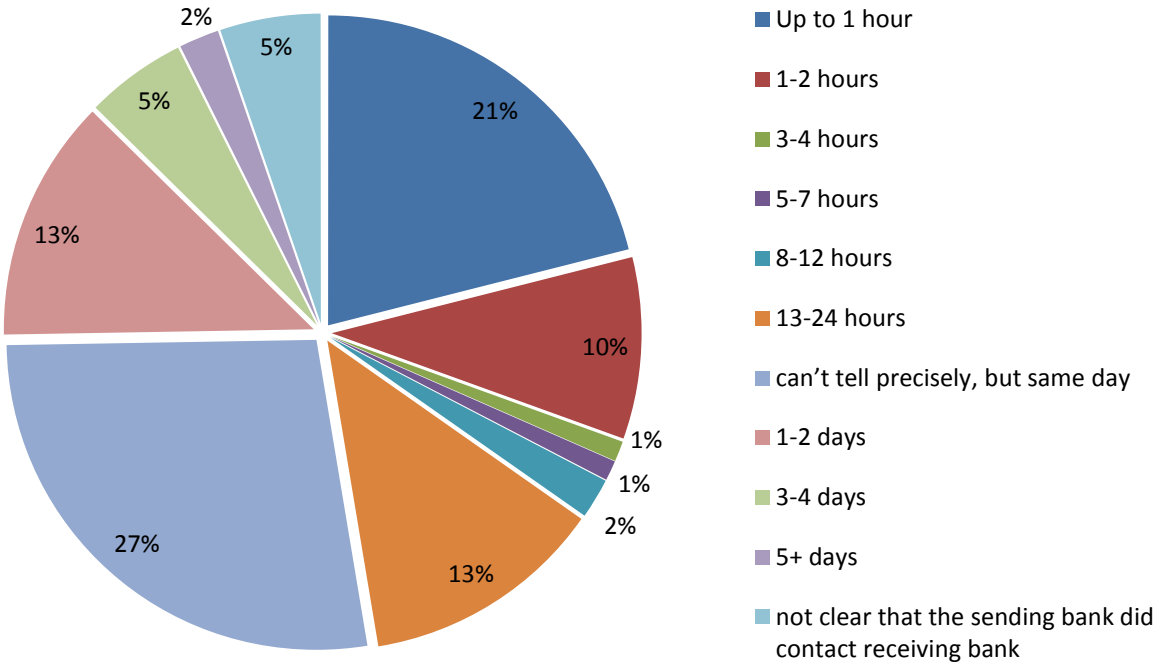
There's no legal requirement on banks to track down money that's been transferred by a consumer during a scam. But it's reasonable to expect a consumer's bank (the "sending bank") to contact the bank where the money has gone (the "receiving bank") to see whether any funds are left – and to ask the receiving bank to block payments out of the account.

speed of banks' response

Our review highlighted variations in how quickly banks responded to instances of no hang-up frauds. In a third of complaints where we were able to identify how long it took the sending bank to contact the receiving bank to attempt to recover lost money, the bank had acted within two hours of learning the consumer had been scammed. One in five banks (20%) acted immediately. And we saw some examples where banks had gone to extra lengths to try to help their customers. In one case where a consumer reported the fraud to their local bank branch, the branch manager even accompanied the consumer on foot to the local branch of the receiving bank to discuss what had happened in person.

But not all banks were so speedy. In about one in three cases (34%) the sending bank took more than 12 hours to contact the receiving bank. In more than one in ten (12%) cases, the sending bank took more than three days to act – or may not even have contacted the receiving bank at all.

figure 4: how long sending banks took to contact the receiving bank



source: Financial Ombudsman Service. Base: 92 individual consumer complaints, where it was possible to establish how long it took for the sending bank to contact the receiving bank.

Disappointingly, even where sending banks acted quickly, in practice this often made little difference to the consumers' chances of getting their money back. In most of the cases we looked at, fraudsters had withdrawn the money before the consumer had even reported the scam. Where we were able to piece together a timeline, the fraudster had accessed the money immediately in almost half (47%) of cases. And in a further 47% of cases the money was withdrawn or transferred to another account by the fraudster on the same day.

If our review is representative of the wider picture, there may be some potential for faster and more coordinated action between sending and receiving banks to help limit the losses of people falling victim to these scams. But given how quickly fraudsters withdraw or transfer the money from the "receiving account", this will always be a challenge.

When a complaint reaches the ombudsman service, we will consider whether the bank's response time is material to the case. Where we find that the actions of the bank caused

unnecessary delays, we might tell the bank to take responsibility for any losses that would have been avoided but for that delay. This could apply both to sending banks and receiving banks, depending on the circumstances.

fraud department opening hours

In their complaints to the ombudsman, a number of consumers raised the issue of the restricted opening hours of their bank's fraud department. They told us about difficulties they'd experienced in contacting the right part of the bank's fraud department at weekends or during the evening. Some people had been told by their own (sending) bank that it couldn't contact the receiving bank's fraud department outside office hours – leading to delays even when the consumer had acted immediately.

> *"[The bank] had nobody available to speak to me either on the same day as the con or in fact for many days after that. Apparently they do not talk to people who have been conned out of money in this way."*
>
> **consumer**

Where fraud line opening hours have been relevant to the complaint, we can look at what happened and consider it as part of the circumstances of the case. Clearly, banks' opening hours are a commercial decision for the businesses concerned. But in a world where online and telephone banking allows customers to make payments at any time of day or night, it's understandable that people might expect to be able to contact their bank – including the right people within its fraud department who can deal with vishing scams, if necessary – around the clock.[15] And in cases where consumers had had difficulty in reaching an appropriate person, we saw how this could often exacerbate an already stressful situation.

clarity and consistency of banks' response

As noted earlier, in the majority of complaints we reviewed (74%) consumers hadn't been able to get any of their money back following the fraud. And where they had, it was rarely more than a small proportion of the money lost. Where banks *had* managed to retrieve some of the money, there were occasionally long delays in returning the funds to the consumer. This sometimes compounded financial problems consumers might have experienced as a result of the fraud.

[15] See, for example, *The Sunday Times*, "Fraudsters profit from delays at big banks", 22 February 2015.

Consumers told us that they felt their bank could have done more to ensure the money was returned to them quickly.

ombudsman case study: slow and confusing response from bank

Mr T received a phone call from "Visa" telling him that there had been fraudulent activity on his debit card. He spoke to someone he thought was at his bank, who asked him to transfer his money to a new, "safe" account.

Mr T transferred tens of thousands of pounds. The following day, he called his genuine bank – and discovered that he'd been the victim of a scam. His bank didn't take any action, although the receiving bank contacted Mr T's bank the following day to raise concerns. Mr T's bank told the receiving bank that a fraud had been reported – and the account Mr T's money was paid into was blocked. However, Mr T's bank didn't request the return of the money in the receiving account for over a week. They also told him he'd get all of his money back.

In fact, only a fraction of Mr T's money remained in the receiving account – and this was returned six weeks after the fraud had taken place. When Mr T brought his complaint to the ombudsman we agreed that the bank could have acted sooner – although it wouldn't have made a difference to the amount of money he got back as the fraudsters had emptied the account the same day. Mr T's bank offered to pay compensation for the distress caused by their delays and misinformation.

The consistency of banks' response was also an issue raised by consumers bringing their complaints to us. Some people had been duped into transferring money from all their accounts – held with different banks. But the different banks had sometimes responded in different ways. For example, we saw cases where consumers had been refunded by one bank but not by another. In some cases where couples had fallen victim together, one partner had been refunded by one bank while the other partner, who banked somewhere else, hadn't.

ombudsman case study: three transfers, three different results

Mr G, who was in his seventies, received a phone call from someone he believed worked in the fraud department of his bank. Having been told his accounts were at risk, he panicked and quickly arranged three online transfers for large sums from a number of his accounts.

One payment was immediately blocked by the security system of the receiving bank concerned. The other two payments went through. "Having had time to think", Mr G called his bank later that evening – and the real fraud department confirmed it had been a scam.

Mr G complained to the banks which had allowed the payments to be processed – explaining that one of his banks had blocked the transaction. Of the remaining banks, one refunded Mr G out of goodwill, and one didn't. Mr G brought his complaint against the third bank to the ombudsman service. We fully investigated the case but had to explain to Mr G that unfortunately, because he had made the payments himself, the loss he had experienced was not the bank's fault. Having considered all the circumstances, we did not feel the bank should refund the money.

The circumstances of a fraud, or the bank's own commercial judgement or policy, might lead a bank to refund a consumer – for example, when the consumer is extremely vulnerable. This is at the discretion of each business, not an obligation. But that in turn can mean it is difficult for consumers to understand why different banks respond differently to seemingly identical (or very similar) frauds.

box 5: the role of the police

Almost all the consumers who contacted us had reported what had happened to the police – often via Action Fraud, the UK's national fraud reporting centre. This information is then sent to relevant police forces across the country to investigate – and will be followed up according to the strength of available leads and the priorities of the individual force. The police have undertaken a range of public awareness-raising work at both national and local level.

Because of the nature of the ombudsman's remit, there was rarely evidence in the complaints we studied to inform this report on whether consumers had managed to get any of their money back following the involvement of the police. But the police told us during our research that a variety of factors combine to make it very difficult to recover money stolen in vishing scams. For those consumers whose bank had not been in a position to stop a transfer being made during a scam, or to recover money afterwards, this could add to the impact of the crime they had suffered.

chapter 7 security and convenience

The balance between security and convenience was a recurrent theme in the complaints we reviewed. In response to customer demand, banks have introduced a number of mechanisms to give people easier access to their money though online, telephone and mobile banking.

> *"...it is for the bank to decide how it scrutinises movements on accounts, and what balance to strike between security considerations and enabling customers to move funds freely."*
>
> **extract from ombudsman final decision**

For example, the Faster Payments Service transfers money from one account to another almost instantly – with funds typically available to the recipient within minutes. Faster Payments have been in use in the UK since 2008. In 2010, transaction limits were increased from £10,000 to £100,000, although not all banks allow this upper limit.[16] The service processes 100 million payments per month and over £900 million was paid using Faster Payments in 2014.[17]

Faster Payments

Banks using the Faster Payments service will check that the request to make a payment is genuine and that there's enough money in the account to cover it. All Faster Payments are sent using just the account number and sort code provided by the person making the payment.

This service has clear everyday benefits to consumers. It was developed to address consumer frustration at the length of time it previously took to transfer money from one bank to another.[18]

However, there is a flipside. Faster Payments are instant and can't be reversed. The payments can't be cancelled after being submitted for processing. In the complaints we reviewed, many of the consumers who'd fallen victim to no hang-up scams felt that their bank should have had

[16] Source: Faster Payments website, www.fasterpayments.org.uk. Information on the different transaction limits applied by banks is available here: www.fasterpayments.org.uk/consumers/transaction-limits.
[17] Source: Payments Council, *Clearing Statistics (Annual) 2014*.
[18] See, for example, "How fast is faster payment plan?", BBC News website, 22 May 2008, available at: http://news.bbc.co.uk/1/hi/business/7411338.stm.

stricter security measures in place. People told us they felt it was "too easy" to transfer very large sums of money without additional layers of protection. But banks that have tried to restrict consumers' access to their money have been criticised.[19]

The consumers who had lost the most money in the complaints we reviewed had been convinced by fraudsters that *all* of their accounts were under threat – and had transferred funds from savings and investments as well as current accounts. With all of their accounts having similar levels of instant access, very large sums of money could be lost in a very short time. The fraudsters then typically use Faster Payments to move the money on quickly to other accounts so that it is out of reach and less easy to trace. This was a particular factor in complaints centring on transfers made online.

Many consumers were surprised that banks only use sort codes and account numbers when making transfers, rather than checking account names. This has been industry practice for some time. The Association for Payment Clearing Services (APACS) – now called UK Payments Administration – published some best practice guidelines for banks in 2007. These say that businesses should make it clear to consumers that the sort code and account number ("unique identifiers") are used to process the payment – rather than the name of the payee, which most businesses don't check. But the experience of the consumers we have heard from suggests that this isn't well understood. This lack of awareness could have provided an opportunity for fraudsters.

ombudsman case study: consumer reassured that destination account is in her name

Ms D received a call one evening from someone she believed to be from her bank. It was in fact a fraudster, who convinced Ms D that her accounts were in danger.

The fraudster gave Ms D the sort code and account number of a "safe account" with another bank – and said it had been set up in Ms D's name. Ms D later told us she was "reassured" by this.

When she discovered she had been scammed, Ms D complained that her bank hadn't made any checks on the name on the "safe" account – which wasn't actually in her

[19] See, for example, "What are you doing with YOUR money? Furious customers hit back at high street banks forcing strict checks on getting out large sums of cash", *This is Money*, 28 January 2014.

name. She said she wouldn't have transferred money to an account that wasn't in her name – and felt that the bank should have warned her that banks don't cross-check names on accounts against account numbers and sort codes. After the complaint came to the ombudsman service, the bank made an offer to Ms D for a full refund.

chapter 8 banks and customer service

When we looked at the reasons why consumers complained to us about a no hang-up fraud, we found that the main drivers were a belief that their bank was responsible for the loss, or could have done more to stop the fraud. But many people were also unhappy with the customer service that banks had provided once they had reported the fraud – something that featured to some extent in a third (34%) of complaints.

> *"I can only compare and contrast the approach of [Bank A] and [Bank B]. [Bank A] has done everything to turn the experience of this terrible fraud into a crisis, whilst [Bank B] has provided excellent customer service all round."*
>
> **consumer**

In fact – taking all aspects of complaints into account – consumers' unhappiness at the customer service they'd received featured more prominently than dissatisfaction with the warnings banks had given, the speed of their response or the actions they'd taken to recover lost money (see table 3).

table 3: reasons for complaining to the ombudsman about a no hang-up fraud

	Main reason for complaint	*All reasons for complaint*
bank responsible for loss and should provide refund	56% (103)	73% (135)
bank could have done more to stop the fraud taking place	21% (39)	45% (83)
bank could have done more to recover the lost funds	7% (13)	20% (37)
consumer unhappy with customer service received	**5% (10)**	**34% (63)**
consumer unhappy with bank's speed of response	5% (9)	12% (22)
bank could have done more to warn consumers	4% (7)	17% (31)
consumer unhappy with operating hours of bank or its fraud team	1% (2)	4% (8)
other	1% (2)	6% (11)

source: Financial Ombudsman Service. Base: 185 complaints, against both "sending" and "receiving" banks.

In the cases we reviewed, we saw some excellent customer care from banks. In particular, we came across many examples of fraud teams acting immediately to try to block the onward transfer of stolen money – and trying to claim it back for the victim.

ombudsman case study: bank acts quickly to fraud alert to protect consumer's money

Mrs L received a series of phone calls about fraudulent activity on her bank account. She put the phone down and rang what she thought was her bank – but fraudsters kept the line open. Pretending to be the bank, the criminals told Mrs L to transfer money to a "safe" account. Believing her funds were at risk, Mrs L made one transfer at her local bank branch and another using telephone banking.

After later speaking to a member of her family, Mrs L realised she'd been duped. She called her bank to report it. They immediately called the bank which had received the fraudulent funds and it was able to block the account. This all happened within minutes of Mrs L's bank being alerted to the fraud. It meant Mrs L was able to get back 70% of her money.

Yet despite examples of good practice by banks after a fraud was reported, we also saw evidence of poor customer service and complaints handling. For example, consumers told us about how anxious they felt waiting to hear back from their bank about whether any money had been recovered from fraudsters – or whether they'd be refunded.

> *"I spent a sleepless night wondering what on earth was going on, and why I hadn't heard anything from the bank."*
>
> **consumer**

It was also clear that consumers' unhappiness with what had happened to them was based on a belief that their bank owed them a "duty of care" due to their loyalty as a customer. Many of the consumers whose complaints we reviewed were from older age groups – and many had been with their bank for decades and considered themselves loyal customers. The length of a time a consumer had banked with a particular institution wouldn't affect the way the ombudsman service handled their complaint: we wouldn't treat a consumer who'd been with their bank for 20 years any differently to one who'd been with their bank for two months. But it's easy to see why the length of relationship could intensify the anger and disappointment some consumers felt.

"I have been a customer of the bank for many years and I believe that entitles me to better treatment than I have received. The bank has failed in its duty of care to me. They know me well in the branch and should have known I would not make withdrawals from my accounts, especially the account I used."

consumer

"My main complaint with the bank is that I was told at least twice soon after the fraud took place that I would almost certainly be refunded as in 95% to 99% of fraud cases this is what happens and, unfortunately, I seem to be in the odd 1% to 5% of cases where this isn't the case!"

consumer

A number of consumers also told us there were delays in the bank communicating with them about what was happening in terms of the recovery of lost money. For many this added stress to an already difficult situation. In other cases consumers told us that when they first reported the fraud, their bank had told them they would be eligible for a refund. However, this initial reassurance wasn't always accurate – with the bank later having to tell the consumer that they wouldn't be refunded after all. In some complaints we asked the bank to pay compensation for the distress they caused through delays and poor communication.

Some consumers were particularly unhappy about the tone of communications they'd received from their bank. Before coming to us, consumers will usually receive a final response letter from their bank in reply to their complaint. A number of people noted that their bank had also enclosed "tips" or leaflets on avoiding fraud with this letter. Consumers described this as "crass" and "insulting" – particularly when the bank had rejected the consumer's request for a refund. One consumer told us that it felt like a "kick in the teeth", while another said: "It's ironic….rather like shutting the door after the horse has bolted." The information will have been well-intended but for those who'd just lost all or most of their savings, it felt like too little too late.

chapter 9 the future of the no hang-up scam – and lessons to learn

the future of the scam

Vishing is just one of many techniques fraudsters use to trick people out of their money. And the no hang-up scam is just one variety of vishing. But from the cases that reach us, it seems a particularly upsetting deception. Consumers believe they're taking quick and necessary steps to keep their money safe in the face of a serious threat of fraud. The reality is the exact opposite.

From the changing nature of the cases we see – and our conversations with businesses and experts – it's clear that fraudsters don't sit still. As efforts are made to tackle one type of scam, new ones emerge. During our review we saw the emergence of new techniques to dupe people on the telephone – including the use of so-called "number-spoofing" where fraudsters impersonate a bank's genuine phone number on the caller ID display of the person they're calling.[20] A number of cases involving this trick have now reached us.

> **ombudsman case study: consumer is duped through "number-spoofing"**
>
> Mrs F took a call on her home phone from someone she believed worked for the fraud department at her bank. She was told that, to confirm the caller's identity, a "colleague" would ring Mrs F's mobile phone with a PIN code. The number that displayed on Mrs F's mobile phone was the correct one for her bank. So Mrs F felt confident she was talking to her genuine bank – and followed the caller's instructions to make an online transfer. It later emerged that fraudsters had used "number-spoofing" technology to impersonate the bank's number on Mrs F's mobile phone.

New variations of "courier fraud" are emerging all the time, with fraudsters impersonating – amongst others – anti-fraud organisations, utility providers, court officials and government departments.[21] In some instances fraudsters, posing as police officers over the phone, are tricking people into buying expensive jewellery, watches and clothing.[22]

---

[20] Financial Fraud Action UK, "Public warned of new "number-spoofing" scam", news release, 29 October 2014.
[21] See, for example: thisismoney.co.uk/money/saving/article-3038971/How-sinister-new-twist-phone-call-scams-cost-Jenny-4-000.html.
[22] Action Fraud, "Alert: Watch out for elaborate forms of courier fraud", press release, 27 January 2015.

There has been an increase in the use of "money mules", where people are either persuaded or duped into allowing their genuine bank account to be used to launder stolen money.[23] Financial fraud experts have also predicted that there will be a rise in the use of malicious software ("malware") and viruses in the future – which fraudsters could use to attempt to infect people's computers and steal information such as banking passwords and other personal details.[24]

Telecoms companies are taking proactive steps during 2015 to remove the facility that enables the no hang-up trick to be carried out on UK landlines.[25] This should help to bring this particular scam to an end. But whether or not vishing persists widely in the future, we think there are a number of broader lessons to be drawn from the complaints we've reviewed that could help increase our collective resilience against fraud.

lessons to learn

The law requires the ombudsman service to decide each complaint we receive on the basis of what we think is fair and reasonable. In complaints about no hang-up scams, our job is to look impartially at what's happened and decide whether the bank should have acted differently and, if so, whether it would have made any difference. However, the nature of the no hang-up scam means that, whether or not we uphold a complaint, the outcome is unlikely to feel fair to the person involved. Many will have lost a lot of money they are unlikely to get back.

From the complaints we've reviewed, we've seen that banks recognise the role they have to play in warning and protecting their customers about fraud. But we found that they're responding in different ways. And when people are customers of more than one bank – or if they've had different experiences in different branches of the *same* bank – this can leave people feeling they haven't been treated fairly. We also found evidence that banks aren't always acting with enough sensitivity when their customers have lost life-changing sums of money.

[23] Cifas (2015), *Fraudscape: UK fraud trends*.
[24] Financial Fraud Action UK, "Scams and computer viruses contribute to fraud increases – calls for national awareness campaign", news release, 27 March 2015.
[25] Ofcom (2014), *Measures helping to foil courier fraudsters*.

These are some areas where we think lessons can be learned from the complaints that have reached us:

❖ warnings

Most banks involved in the complaints we reviewed had issued warnings about no hang-up and similar frauds in a variety of formats and mediums – both physical and digital. But these warnings hadn't been issued in the same way and at the same time to all customers.

There's no guarantee that warnings will be effective in preventing scams taking place – and some banks told us how they were trying to make their warnings more sophisticated and targeted. Even so, more consistent practice across the banking sector could help to embed the message for consumers. Recent examples of banks and the police working together seems a step in the right direction.[26]

❖ Faster Payments

Most of the incidences of no hang-up fraud that we've seen have relied on Faster Payments. This is the simplest and quickest way for a fraudster to get hold of money as payments are instant and can't be reversed. The fraudsters can also use this method to disseminate funds to other accounts – all within minutes in many cases. Many of the victims felt it was "too easy" to transfer significant sums of money without additional layers of protection.

Our review also found that not all consumers are aware of the fact that Faster Payment transfers are made using only sort codes and account numbers – not the name of the recipient account holder. The fact that this isn't very well understood by consumers might make these frauds easier to perpetrate.

❖ in-branch prevention

Where frauds involve a visit to a bank branch, there's greater opportunity for the bank to identify and prevent fraud. We saw good examples of this in our review. But in some of the cases that have come to us, bank staff suspected that fraud was taking place – and still allowed withdrawals or transfers to go ahead. The complaints we have reviewed suggest there is room

[26] Financial Fraud Action UK, *Joint declaration – phone scams,* 1 December 2014.

for improvement in bank procedures here. But we recognise that the balance between security and convenience remains a fine line for banks to tread on behalf of their customers.

❖ effective complaint handling

Banks can help consumers who've fallen victim to no hang-up scams – or other types of fraud – simply by being sympathetic and helpful. In too many of the cases that reach us, the consumer's situation has been made more stressful and difficult by the way their bank has handled their complaint. In particular, we heard from many consumers who were unhappy about delays in communication and about the tone of the final response letters they'd received.

❖ consumers

Advances in banking security systems mean it's likely that fraudsters will target consumers as the "weak link" in the security chain. This makes it essential that consumers are aware of the risk of fraud – and take notice of the messages that banks and the police issue about never giving details over the phone or transferring money to a different account. We have included some advice on how to avoid scams at the end of this report.

final word

Fraudsters' approaches are continually evolving. And with recent changes to pension rules allowing people to access substantial sums of money, concern about financial fraud remains high.[27]

The ombudsman service hears both sides of complaints. This gives us a unique perspective. We only see part of the picture. But we hope that what we've shared will help businesses in their ongoing efforts to protect consumers – and to reflect on some areas where their response to complaints has fallen short in their customers' eyes. And we hope that our insight will complement the efforts of others in helping to raise consumers' awareness of the risks they face.

[27] Financial Conduct Authority, "As new pension freedoms arrive be ScamSmart", News Release, 23 March 2015.

We'll be playing our own part by working closely with a range of organisations in this shared fight against fraud – to help keep people, and their money, safe.

avoiding scams – hints and tips

There are many different scams – but just a few general hints and tips can help you protect yourself against many of them:

- never give out your personal or banking information in response to an incoming call – and remember that the number on your phone's "Caller ID" may not be the number that's really calling.
- instead, hang up and call the phone number for your bank on a recent statement, in the phone book, or on the bank's website (or if it's another service, their own website) – to check whether the call was genuine.
- *wait at least five minutes* before making the call or use a different phone – to ensure you avoid the "no hang-up" trick and don't end up speaking to fraudsters again.
- protect your financial details by getting into the habit of shredding old bank statements, receipts and other documents containing any financial information like account numbers.
- remember, if your bank suspects your account has been compromised by fraudsters they will usually 'freeze the account' which will prevent any transactions happening – there is no need for you to do anything.

Remember, your bank or the police will *never*:

- ask you to authorise a money transfer to a new account – or to hand over cash.
- ask for your full PIN or any online banking passwords over the phone or by email – including asking you to put your PIN into your phone's keypad.
- send someone to your home to collect cash, bank cards or anything else.
- ask you to email or text personal or banking information.
- send you an email with a link to a page which asks you to enter your online banking log-in details.
- call to advise you to buy diamonds, land or other commodities.
- ask you to carry out a "test transaction" online.
- provide banking services through any mobile apps other than the bank's official apps.

annex about the ombudsman

- We were set up under the *Financial Services and Markets Act 2000* to resolve individual complaints between financial businesses and their customers – fairly and informally.
- We can help with concerns and complaints about all kinds of money matters – from insurance and mortgages to savings and payday loans.
- Our service is free to consumers.
- If a financial business can't resolve their customer's complaint, we can step in. But the business must have the chance to sort things out first.
- We're independent and unbiased. We listen carefully to different perspectives – look at the facts about what's happened – and find a way forward that helps both sides move on.
- If we decide that a business has acted fairly, we'll explain why. But if we decide they've acted unfairly, we'll use our power to put things right.
- Consumers don't have to accept our answer about their complaint. But if they accept an ombudsman's decision, it's binding both on them and the business.
- We don't write the rules for financial businesses – or fine them if rules are broken. That's the job of the regulator.
- Everyone can learn something from complaints – so that what's gone wrong in the past doesn't happen again. So we're committed to sharing our insight to help make money matters fairer.