

ombudsman news

essential reading for people interested in financial complaints – and how to prevent or settle them

in this issue

complaints involving
scams

page 3

ombudsman focus:
spotlight on scams
page 17

Q&A **page 26**

fighting fraud

Money matters are complicated enough to navigate, without the risk of falling victim to financial crime. Unfortunately, scams are a fact of daily life – and when daily life changes, scams evolve with it.

In particular, new technologies – which should make life easier – inevitably come with new risks. So while some people continue to receive fake investment opportunities through their letterbox, others are falling victim to “number spoofing” on their mobiles – or finding their online business banking threatened by malware.

Our case studies in this issue echo many of the problems I heard about at a recent drop-in we held with MPs and their caseworkers.

Regardless of the type of scam – or the amount of money that’s been lost – the ordeal of being scammed may be distressing, and even life-changing. From our conversations with financial businesses, we know that protecting customers is high on their agenda. And it makes sense that part of the solution will be ensuring that technology and other safeguards keep one step ahead of the scammers.

But in the face of ever-more sophisticated crime, what else can be done? Like so many other financial problems, awareness plays a huge role in prevention. So to me, it’s essential that everyone with an insight, shares that insight. That goes as much for individual people talking to their neighbours as it does for organisations like ours – who, in dealing with large volumes of complaints and concerns, can see the bigger picture and identify worrying patterns and trends.




Financial
Ombudsman
Service



follow us

 @financialombuds  Financial Ombudsman Service

 financial-ombudsman.org.uk

subscribe ombudsman.news@financial-ombudsman.org.uk

meet us we're in:

- ◆ Glasgow
- ◆ Sheffield

for dates see page 25



scan for
previous issues



Caroline Wayman

At the ombudsman, we'll continue to share what we're seeing whenever we can – as we did with our report on phone fraud last year. And I'm grateful to the experts who've shared their perspectives with us in this month's *ombudsman focus*.

By keeping up the conversation about scams, and working together, we can all play a part in stopping them.

Caroline

... it's essential that everyone with an insight shares that insight

Financial Ombudsman Service

Exchange Tower
London E14 9SR

switchboard 020 7964 1000

consumer helpline

Monday to Friday 8am to 8pm *and*
Saturday 9am to 1pm

0800 023 4 567

technical advice desk

020 7964 1400

Monday to Friday 9am to 5pm

© Financial Ombudsman Service Limited. You can freely reproduce the text, if you quote the source.

ombudsman news is not a definitive statement of the law, our approach or our procedure. It gives general information on the position at the date of publication. The illustrative case studies are based broadly on real life cases, but are not precedents. We decide individual cases on their own facts.

complaints involving scams

With losses from financial fraud increasing significantly over recent years – both for businesses and their customers – it’s perhaps not surprising that we continue to see complaints involving a range of scams. And as with many of the problems people bring to us, scams can have a huge personal impact on people’s lives – with some people losing their life savings.

Some scams – including in areas where we’ve previously shared our insight – have become less common in recent months, thanks to new technology and increased awareness. But scams and fraud continue to develop – and the following case studies highlight the range of problems we see.

In some cases of fraudulent investments, scammers pose as legitimate regulated businesses to trick people into transferring them money. In these cases, we may be unable to help, since the person isn’t dealing with a regulated financial business. The Financial Conduct Authority (FCA) has information on these “clone” firms – and how to avoid them – on their website, along with wider information on how to avoid scams.

case study 135/1

consumer complains that payment provider didn’t offer enough protection after scam leaves her without goods or payment

Ms B was selling her mobile phone online, and used an electronic payment provider to receive the buyer’s payment. After the buyer had sent her £200, they asked to collect the phone in person.

A week later, after the buyer had collected the phone, Ms B received an email from the payment provider. They said the payment she’d received for the phone had been fraudulent – and they asked for proof of postage to check the phone had been sent to the buyer.

Ms B told the payment provider the buyer had collected the phone in person, so she didn’t have proof of postage.

In response, the payment provider said since she hadn’t posted the phone, she wasn’t covered by their protection policy – so they couldn’t refund the money she’d lost.

Unhappy with the payment provider’s decision, Ms B complained. She said she’d been left without a phone or any payment – and their protection policy should have covered her for these kinds of situation. And when the payment provider wouldn’t change their decision, Ms B called us.

complaint not upheld

We asked the payment provider for more information about Ms B’s complaint. They explained that Ms B had been the victim of a scam, as someone had fraudulently used the buyer’s account to purchase the phone.

... the payment provider explained that Ms B had complained about a similar scam a few years earlier

When the real account holder had queried the payment, the payment provider had carried out a full investigation – and they sent us evidence showing that the account holder hadn't authorised the payment.

The payment provider also sent us a copy of their user agreement. The agreement showed that a seller would only be protected if they could provide proof they'd sent the item to the buyer's listed address – which Ms B hadn't done.

When we asked if Ms B had been made aware of this, the payment provider explained that Ms B had complained about a similar scam a few years earlier. On that occasion, they'd refunded Ms B as a gesture of goodwill – but they'd highlighted the relevant parts of their user agreement at the same time. So they said Ms B would have been aware she wouldn't be protected if she couldn't provide proof of postage.

Ms B accepted that she'd been told she wouldn't be protected if she delivered an item in person. But she said she thought the payment provider's terms were unfair – and since she'd lost out, she wanted them to cover the cost.

We explained to Ms B that it's not for the ombudsman to tell the payment provider what procedures or practices it should follow. From the user agreement, it was clear this kind of scam wasn't covered – and we thought the payment provider had applied their terms fairly. While we were sorry to hear that Ms B had lost out to a scam, we said the payment provider had acted fairly.

case study 135/2

consumer complains that business should help after losing €500 to scam firm

Mr K received a phone call from a man claiming to be from an investment company, Company A. He told Mr K his company dealt in derivatives, and said Mr K could make significant returns if he was willing to invest straightaway.

After some discussion about the details – and having looked at the company’s website – Mr K agreed to transfer €500 to the investment company. But when it became clear some time later that his money hadn’t been invested as it should, Mr K found an address for Company A and wrote to complain.

The owner of Company A wrote back to Mr K saying she’d never received any money from him.

She said she didn’t know who he’d sent his money to, but since it wasn’t her company, she wouldn’t be refunding his money.

Frustrated, Mr K asked us to step in.

complaint out of jurisdiction

We spoke to Company A about the money Mr K said he’d transferred. The owner told us she was the only person in the business who would deal with customers directly over the phone, and she’d never spoken to Mr K. She explained that her company didn’t have an active website – and the account Mr K had transferred money to didn’t belong to her business.

It was clear that a scammer had posed as Company A to trick Mr K into transferring money. We explained to Company A that a scammer had used their details to create a “clone” firm – and we encouraged the owner to report the matter to the regulator and the police.

Looking at the website Mr K had been directed to by the scammer, we agreed it looked very professional – and even included the regulator’s Firm Registration Number for Company A. So we appreciated that he genuinely believed he’d been dealing with a regulated investment company.

But we explained that we could only look into complaints from customers of regulated financial businesses – and since Mr K wasn’t a customer of the real Company A, we couldn’t deal with the complaint against that firm.

We were sorry to hear that Mr K had lost money, and we encouraged him to report the scam to the regulator and the police. And Company A’s owner contacted us to let us know that since she’d reported the scam, the regulator had issued a warning – and two potential investors had avoided losing money after being contacted by scammers.

... she’d reported the scam, the regulator had issued a warning – and two potential investors had avoided losing money after being contacted by scammers

case study 135/3

consumer complains that bank won't refund money transferred to computer scammers

Mrs N received a phone call from someone who said they were from her broadband company. Mrs N said her computer had been running slowly, and agreed to let the caller access her PC remotely to make it run faster. Half an hour later, while Mrs N was still on the call, the caller offered her £200 compensation, and asked for her bank details to make the payment.

After a few more minutes, they said they'd fixed her PC. But they said they'd accidentally paid £3,200 into her bank account – and as it would take a day to reboot her PC, they asked her to visit the post office in the meantime to send them the money they'd overpaid.

Mrs N went to her post office and arranged a money transfer with her debit card. But as she was walking home, she began to have concerns about what she'd been told. Worried she could have been scammed, Mrs N called her bank as soon as she reached her house.

The bank's adviser established that Mrs N hadn't given the caller the reference number needed to receive the money she'd transferred. And they told Mrs N that, if she had concerns, she would need to go back to the post office.

Later that day, Mrs N called the bank again. She said the caller had just phoned back and convinced her to give them the reference number they needed. And having checked her accounts online, she'd realised that the £3,200 they'd told her had accidentally been paid into her account had actually been moved from her savings account – so she'd sent the scammers £3,000 from her own savings.

The bank's adviser made enquiries with their fraud team – and eventually told Mrs N that they couldn't reverse the transaction.

Mrs N complained to the bank. She said if the bank had checked her bank accounts – and clearly told her she'd been scammed – she wouldn't have given the scammers the transfer reference number.

The bank offered Mrs N £50 to recognise that their customer service could have been better. But unhappy with this – and distressed at the prospect of losing so much money – she phoned us.

complaint resolved

We asked the bank for recordings of Mrs N's calls to them – so we could establish whether they'd done enough to stop Mrs N losing her money.

It seemed that when Mrs N had first called the bank, she'd gone into a lot of detail about what had happened. She'd explained that the caller had told her to log on to her online banking while they were accessing her PC – and that she'd seen the £3,200 in her account.

In our view, the adviser hadn't sounded sympathetic at all. At one point, he told Mrs N that no one could have accessed her computer. And when she'd raised concerns about transferring her money through the post office, he'd assured her that the transfer "would have been legitimate".

We also listened to the adviser's conversation with the bank's internal fraud team. Despite Mrs N having clearly described what she'd done, the adviser appeared not to have listened – telling the fraud team she'd "bought something she didn't want".

When Mrs N phoned the bank after giving the scammer the reference number, the person she spoke to was far more helpful. He said that he'd heard about these types of scams – and acknowledged that someone could have accessed Mrs N's PC.

He then made several internal phone calls to see if there was anything the bank could do to get the money back – clearly explaining to his colleagues what had happened to Mrs N. But by this time, it was too late for the bank to stop her money being moved.

The bank told us that, while they had sympathy with Mrs N, she shouldn't have given the scammer the transfer reference number if she'd had concerns. They also said they gave scam warnings when customers logged in to online banking.

We appreciated that, at least later on, the bank had tried to help Mrs N. But we thought that the bank could have done more during the first phone call – and that if they had, it was likely that Mrs N wouldn't have lost her money.

In particular, we pointed out that the first adviser's lack of clarity and empathy – when she'd made it clear what her state of mind was – had left Mrs N with doubts about whether or not she'd actually been scammed.

And he hadn't looked into her account activity. We agreed with Mrs N that, if he'd told her the money in her bank had in fact come from her savings account, it would have confirmed to her that something was wrong.

In the circumstances, the bank offered to cover the £3,000 Mrs N had lost – and to pay her £200 to reflect the poor service she'd received from them.

... as she was walking home, she began to have concerns about what she'd been told

▶

case study 135/4

consumer complains after insurer won't pay out for watch sent to scammer

Mr Y sold his watch through an online auction site. After he received payment, the buyer contacted him, asking for the watch to be sent to a different address to the one he'd listed on his online profile.

After Mr Y had posted the watch, he received an email from the auction site. The email said the payment he'd received for his watch hadn't been authorised – so the money he'd received would be refunded to the account the payment had come from. And since he hadn't sent the watch to the address listed online, he wasn't covered by the auction site's own protection scheme – and he couldn't get a refund for the watch.

Left without his watch or payment, Mr Y contacted his home insurer. He said the scammer had stolen his watch, and he wanted to make a claim. But the insurer said Mr Y had willingly posted the watch – and as soon as he'd posted it, he no longer owned the watch. So it couldn't have been stolen from him.

Mr Y complained. But when the insurer maintained they wouldn't pay the claim, Mr Y brought his complaint to us.

complaint not upheld

We asked Mr Y for more information about what had happened. He said he'd never sold anything online before, so he hadn't been suspicious about the change of address. And when he realised he'd sent the watch to a fraudster, he'd done all he could to stop the post – but he'd been unsuccessful.

Mr Y also told us he was aware of a similar court case which suggested his watch had been stolen – so he felt he should be able to claim under the policy.

In the circumstances, we agreed that Mr Y's watch had been stolen. But the insurer said that even if the watch was stolen, their policy didn't cover theft by deception – and since the scammer had clearly deceived Mr Y to get the watch, the claim wasn't covered.

Mr Y said this was the first he'd heard of this exclusion – and he didn't think it was fair that the insurer hadn't mentioned it in their final response letter about his claim. But listening to the calls Mr Y had made to his insurer, they had clearly discussed the “theft by deception” exclusion – and why Mr Y wouldn't be covered under those circumstances.

We appreciated that the insurer's letter to Mr Y hadn't specifically mentioned theft by deception. And we thought they could have explained their position more clearly in that letter. But they had been clear when they spoke to Mr Y on the phone. So while we were sorry to hear that Mr Y's watch had been stolen, we didn't tell the insurer to pay the claim.

... the insurer said Mr Y had willingly posted the watch – and as soon as he'd posted it, he no longer owned the watch. So it couldn't have been stolen from him

... one of the online warnings the bank told us about said that a slow-running website could indicate possible fraud

case study 135/5

small business complains that bank won't refund fraudulent transactions – after employee uses hoax website following malware attack

One afternoon one of Mr G's employees, Miss O, told him that she thought there'd been fraud on his business's bank account.

Miss O said she'd been using the online business banking service and had been prompted to enter the log-in details. A short time later, she'd noticed that around £40,000 had been paid from the account to payees she didn't recognise.

Mr G phoned his bank immediately to explain what had happened. They said it was likely that the computer Miss O had been using was infected with a virus – and that the screen she'd seen was a hoax

page. In putting in the details, she'd inadvertently given the fraudsters what they needed to take the money.

Mr G's bank raised an indemnity claim with the banks that the money had been transferred to – but only managed to recover around £2,000 of more than £40,000 that had been lost.

When Mr G asked his bank to cover the rest of the money, they refused. They said his business had broken the terms and conditions of the account – acting with “*gross negligence*” by giving the passcode to a third party.

Frustrated, Mr G complained. When the bank wouldn't reconsider, he contacted us.

complaint upheld

We asked the bank for the terms and conditions they were referring to. These didn't say that a business would be responsible for any losses arising from the log-in details being disclosed to a third party. However, we considered whether Miss O had authorised the transactions – which might have meant the business was liable for them.

Looking at what had happened, it seemed that although Miss O had typed in the business's passcode, the fraudsters had gone on to make the transactions themselves. So Miss O hadn't actually authorised the transactions. The bank also acknowledged that the hoax website would have looked exactly like their own – so Miss O couldn't have known she was using a fake site. In the circumstances, we didn't agree that she'd been grossly negligent.

The bank told us that they gave security warnings on their business banking website explaining the risk of fraud. They argued that Mr G and his employees should have read these.

But according to Mr G – and the bank's records – Miss O had phoned the bank shortly before she reported the missing money, to say the website was running slowly. The bank's adviser had told her there was nothing wrong and that she could carry on using the site. Yet one of the online warnings the bank told us about said that a slow-running website could indicate possible fraud.

We pointed out to the bank that – as malware was a problem that the bank was actively warning its customers about – we thought their adviser could have alerted Miss O that something might be wrong.

Given everything we'd seen, we decided the bank could have done more to prevent Mr G's business from losing their money – and told them to cover the amount they hadn't been able to get back.

... the investment provider had told the adviser they couldn't trace the solicitor's firm, so they wouldn't transfer the money to the account

case study
135/6

consumer complains that adviser won't pay back money transferred to fraudsters from investment bond – after her email was hacked

Ms Q received a letter from the provider of her investment bond, confirming £250,000 had been withdrawn. But she hadn't made a withdrawal. Shocked, she phoned her financial adviser – who said he'd processed the transaction after arranging it with her by email.

Ms Q and the adviser established that her email account must have been hacked. So the emails the adviser had received had been coming from Ms Q's address, but she hadn't sent them herself. And the bank account the fraudsters had given to transfer the money to – although in Ms Q's name – wasn't actually her account.

After reporting the fraud to the police, Ms Q managed to recover around £170,000. But she felt the adviser should have checked before arranging the withdrawal – and asked them to make up the money she hadn't got back.

The adviser said they couldn't have known the emails weren't really from Ms Q. But to settle her complaint, they offered to pay 25% of the money she'd lost.

Ms Q didn't think this was enough – and contacted us.

complaint upheld

We asked the adviser to send us the emails they'd exchanged with the fraudsters who were pretending to be Ms Q – as well as the adviser's records of their contact with the investment provider.

We saw that the fraudsters had initially provided details for a solicitor's bank account in Hong Kong. The investment provider had told the adviser they couldn't trace the solicitor's firm, so they wouldn't transfer the money to the account.

The adviser had emailed "Ms Q" to let her know – and "Ms Q" had replied with details of an account in her name, with a UK high street bank. In processing this second request for the funds to be withdrawn, the investment provider highlighted that the account details were different to what they had on their records for Ms Q. But the adviser confirmed the details were correct – and finalised the transaction.

Ms Q told us that she'd used the same financial adviser for more than ten years and always had a face-to-face meeting when she wanted to discuss her investments. So she thought the adviser shouldn't have acted without phoning her first.

For their part, the adviser said that, around that time, Ms Q had been emailing them about arranging a mortgage. So getting an email from her wasn't unusual – or cause for concern. They also pointed out that Ms Q had worked in Asia in the past, so it seemed reasonable that she'd want to use a Hong Kong bank account.

Given everything we'd seen, we agreed with Ms Q that the adviser should have taken more care of her money.

We acknowledged that Ms Q had emailed the adviser before – and that she had worked in Asia. But as a finance professional, the adviser would have been aware of the risk of fraud and scams. And in our view – having received an email asking for such a large sum of money to be transferred overseas – the adviser could have realised something wasn't right.

If that wasn't enough, we thought alarm bells should certainly have started ringing when the investment provider said they couldn't trace the firm of solicitors. We found it hard to see why, at that point, the adviser hadn't phoned Ms Q.

All in all, we decided the adviser could have stopped the fraud happening. The investment provider had already adjusted Ms Q's bond when she'd recovered some of the money. So we told the adviser to pay the provider the amount needed to put Ms Q's bond in the position it would be in if the unrecovered money hadn't been stolen.

case study 135/7

consumer complains after insurer rejects claim for car stolen during test drive

Mr C was selling his car online. When a man responded to his advert, Mr C arranged to show him the car. But while Mr C was showing the man the car, the man stole it.

Mr C called his insurer to make a claim. But the insurer told him they wouldn't pay out, as his policy didn't cover theft where someone was posing as a buyer in order to steal the car.

Mr C complained. He said he didn't remember ever having been told about the exclusion, so he didn't think it was fair for the insurer to rely on it to turn down his claim. And in any case, he didn't agree the man was a "buyer", since he hadn't ever agreed to buy the car.

When the insurer maintained their decision, Mr C referred the complaint to us.

complaint not upheld

We asked Mr C for more details about the theft. He explained that he'd invited the man to a nearby car park so he could see how well the car drove. The man said the car drove really well. As Mr C got out of the car to swap sides – leaving the keys in the ignition and the engine running – the man stayed in the driver's seat. While Mr C was walking around the car, the man shut the driver's door and drove away.

Looking at Mr C's policy documents, the policy said theft "resulting from deception by a person pretending to be a buyer" wouldn't be covered. And we could see this was listed clearly as an exclusion in the policy summary – so we thought the insurer had highlighted the exclusion to Mr C.

Mr C accepted that he'd been told about the exclusion, but he didn't think it was relevant in his circumstances. He said that as the policy didn't define a "buyer", it must refer

to someone who bought, or agreed to buy, the car. He agreed that the man had tricked him. But in his view, the man had never agreed to buy the car – so he couldn't have been a "buyer".

We didn't agree. It was clear from the man's actions that he'd set out to trick Mr C – and he'd done so by pretending to be interested in buying the car. And even though he hadn't actually made an offer for the car, the man was clearly posing as a potential buyer – so the policy was clear that Mr C wouldn't be covered.

While we were sorry to hear that Mr C had lost his car, we thought the insurer had applied the exclusion fairly – and we didn't tell them to pay the claim.

... he'd set out to trick Mr C – and he'd done so by pretending to be interested in buying the car

▶

case study 135/8

consumer complains that insurer won't pay claim following alleged "crash for cash" scam

Mrs E was driving to work with a friend when she drove into the back of another car. She claimed on her car insurance, saying the driver had deliberately braked and that she'd been the victim of a "crash for cash" scam.

The insurer sent an engineer to inspect Mrs E's car – who concluded that she had caused the accident. When Mrs E complained, the insurer said that if the other driver withdrew their claim against Mrs E, they'd make sure her no-claims discount reflected the fact the accident wasn't her fault.

But the insurer explained to Mrs E that the other party was in the process of gathering evidence about the accident. And they said if the evidence was strong, the claim might eventually be settled as a "fault claim" against Mrs E.

18 months later, Mrs E was still waiting for an answer – and complained again. The insurer apologised, saying they'd already settled the claim. And unhappy with their offer of £50 compensation, Mrs E contacted us.

complaint upheld

The terms and conditions of Mrs E's insurance policy clearly said the insurer could decide whether or not to accept liability for any accidents. We explained to Mrs E that this was normal in car insurance. But we would check the insurer had acted fairly in her individual circumstances.

When we asked for the insurer's records, we found that the other party had claimed for personal injury resulting from the accident.

Mrs E's insurer had initially rejected the claim – but had later settled it. However, the insurer hadn't told her about this.

We also had concerns about how the insurer had looked into Mrs E's case. In particular, there was no evidence they'd asked Mrs E's passenger about how the accident happened. In our view, given Mrs E seemed to feel strongly that she'd been a victim of a scam, the insurer could have investigated more thoroughly.

In light of what we'd seen, we decided that – even though it was the insurer's call whether to defend the other party's claim – £50 didn't make up for their poor customer service. We told them to pay Mrs E another £250 for the upset and inconvenience she'd experienced because of their poor communication and handling of the claim.

... given Mrs E seemed to feel strongly that she'd been a victim of a scam, the insurer could have investigated more thoroughly

... the fraudsters had used a technique known as “number spoofing” to make it appear that they were calling from his bank

case study 135/9

consumer complains that bank should refund fraudulent transfer

When Mr M’s phone rang, his phone showed the call was from his bank. The person on the phone told him some money had been taken from his account.

After a lengthy discussion about his account details – answering various security questions along the way – Mr M was told his account had been temporarily blocked, and he wouldn’t be able to use his online banking. He arranged to meet a manager at his local branch the next day, in order to reactivate his account.

But when Mr M arrived at his local branch the next day, he found the branch was closed for a bank holiday. When he called his bank, they said it seemed he’d been the victim of a scam. They confirmed almost all the money in his account had been taken – totalling around £15,000.

The adviser said the bank would do all they could to get the money back. But when they told him two weeks later they’d only managed to recover £10, Mr M complained.

Mr M said the bank’s customer service had been terrible, and he wanted a refund of all the money he’d lost. But the bank said he’d authorised the transfer himself – so they weren’t responsible. Frustrated, Mr M called us.

complaint upheld in part

We asked Mr M for more information about the phone call he’d thought was from his bank. Mr M told us he’d been called on his mobile – and the number on the screen was his bank’s phone number. He’d only later discovered that the fraudsters had used a technique known as “number spoofing” to make it appear that they were calling from his bank.

Mr M explained that he’d given the person on the phone some details, including a security code from his card reader. He said that, other than the code, the only personal details he’d provided were his date of birth and mother’s maiden name.

But the bank explained that Mr M’s money had been sent from his online bank account – and they confirmed the fraudster would have needed Mr M’s username and password to gain access to the account.

When we spoke to Mr M about this, he said the phone call from the fraudsters had lasted some time – and on reflection, he couldn’t remember exactly what details he’d given out. Given that the fraudsters would have needed Mr M’s security details to access his account, it seemed they must have persuaded him to provide this information over the phone.

We thought that by voluntarily giving the fraudsters his security details, Mr M had effectively authorised the transfer himself – so we didn’t tell the bank to refund the money.

But looking at the bank’s response to the scam, it was clear they could have provided better service to Mr M. He’d called them several times, and each time an adviser had promised to call him back – but no-one had done so. Mr M was already very upset and stressed – and the bank’s lack of response had only added to that stress.

The bank agreed with us that their service had fallen short of their usual standards. They offered Mr M £200, which he accepted.

... he'd taken a risk in entering his PIN without being able to see how much money he was agreeing to pay

case study 135/10

consumer complains after bank refuses to refund fraudulent transaction while on holiday

Mr V was shopping on holiday abroad. When the shopkeeper offered him a mobile phone that would give him unlimited calls and internet access for £10 per month, Mr V agreed to buy it.

The shopkeeper told Mr V he'd set up a direct debit for the monthly fee, with no upfront cost for the phone. But when he returned to the UK, Mr V discovered that £8,000 had been debited from his account – so he contacted his bank immediately asking for the money to be refunded.

When the bank said they couldn't get the money back, Mr V complained. He insisted he hadn't given permission for so much money to be taken from his account.

But when the bank said he must have authorised the transaction – and maintained they wouldn't refund the money – Mr V brought his complaint to us.

complaint not upheld

We asked Mr V for more details about the transaction. Mr V said he'd put his card into a payment terminal with a blank screen. He said he'd been suspicious at first – but when he queried the blank screen, the shopkeeper explained that it was a special function for direct debits. The shopkeeper had reassured Mr V that no money would be taken at that time – so Mr V had entered his PIN into the terminal.

When we spoke to Mr V's bank, they told us they'd attempted to get his money back through a "chargeback" – asking the shopkeeper's bank to return the money – as soon as he'd contacted them. But the other bank had successfully defended the chargeback.

And since Mr V had entered his PIN voluntarily, the bank maintained he'd authorised the transaction – and they said there was nothing more they could do to get the money back.

Mr V accepted that he'd put his security details into the payment terminal. But he said he hadn't been authorising such a large payment – so he still thought his bank should refund the money.

Looking at what had happened, it was clear Mr V had been tricked into making the transaction. But he'd taken a risk in entering his PIN without being able to see how much money he was agreeing to pay.

In the circumstances, we took the view that Mr V had authorised the payment. And while we were sorry to hear that he'd lost a lot of money, we didn't tell the bank to refund him.

135/11

consumer complains that insurer won't pay for antique brooch stolen by dealer

Mr L arranged for an antiques dealer to visit his home to value a gold brooch. He gave the dealer the brooch to sell at auction – but when he later tried to contact the dealer to find out what had happened, they wouldn't answer their phone and their website had gone.

Mr L claimed for the brooch on his home insurance. But the insurer turned down the claim – saying they wouldn't pay for items that had been lost “by deception”.

Mr L argued that he'd been put in touch with the dealer through a legitimate auction house. He didn't agree he'd been deceived into giving the brooch to the dealer – saying it was only later on that it became clear the brooch had been stolen.

But the insurer wouldn't change their decision – and Mr L contacted us.

complaint not upheld

We looked at the terms and conditions of Mr L's insurance policy. This said that the insurer wouldn't cover “*loss by deception, unless the only deception used is to get into your home*”.

Mr L had asked the dealer to visit his home, so he hadn't been deceived in that way – but we still needed to decide whether he'd lost the brooch by deception.

Mr L told us that the dealer had since been arrested – after deliberately closing his business and “absconding” with more than 500 other items. In this light, it didn't seem the dealer had ever intended to sell the brooch.

On the other hand, the dealer had told Mr L he would take it to an auction. In our view, Mr L had been deceived.

Mr L felt the insurer should have told him they didn't cover this type of claim. However, we explained that this type of exclusion is usual in home insurance policies. And there was nothing about Mr L's circumstances that suggested he wouldn't have bought the policy if he'd known about the exclusion.

We were sorry to hear what had happened to Mr L – but we decided the insurer hadn't acted unfairly in turning down his claim.

... the dealer had since been arrested – after deliberately closing his business and “absconding” with more than 500 other items

case study 135/12

consumer complains that credit card provider won't pay section 75 claim for scam "investments"

Following a cold call from a marketing company, Mrs A agreed to pay £10,000 to Company D – believing her money would be invested in forestry schemes.

A few months later – after receiving a cheque for around £200 – she complained that she hadn't got the level of return she'd been promised. Although Company D repeatedly told her she'd receive more money, it didn't arrive. Unhappy, Mrs A contacted the provider of the credit card she'd used to put down an initial payment – and asked if they could get her money back.

The credit card provider looked into the claim. But they told Mrs A she didn't have a valid claim under section 75 of the *Consumer Credit Act* – because there was no "debtor, creditor, supplier" chain. They said that, although she'd made the payment to Company D, the company that ran the forestry scheme – Company E – was the one she actually had the contact with. And Companies D and E didn't have any connection with each other.

The credit card provider also pointed out that Mrs A hadn't ever been guaranteed a return on her investment. So they didn't think there had been any breach of contract.

Unhappy, Mrs A complained – and the dispute was eventually escalated to us.

complaint upheld

First, we needed to establish who exactly Mrs A had a contract with. So we looked carefully through the paperwork Mrs A had been sent about the supposed investment.

In our view, the documents were very unclear – and contradictory in places.

However, at various points, Company D and Company E were referred to as jointly and severally liable for the completion of the contract.

We told the credit card provider that, from what we'd seen, we'd concluded Company D was a "supplier". So there was a valid "debtor, creditor, supplier" chain – and it was irrelevant whether Company D and Company E were related.

Mrs A sent us information she'd received from the police, who she'd also been in touch with. The police said that they believed the "investment" was a boiler room scam – and that around 500 other people were in a similar position. They didn't think anyone's money had actually been invested, but that small payments had been made to give the impression that it had.

We also found that Company D's website had been taken down – and that Company D had been struck off the Companies Register.

In light of everything we'd seen, we decided it was likely that Mrs A's money hadn't been invested – which meant that Company D had breached their contract with her. So we told the credit card provider to refund the £10,000 she'd paid.

... they didn't think anyone's money had actually been invested, but that small payments had been made to give the impression that it had

ombudsman focus: spotlight on scams

Last year £775 million was lost to financial fraud (*Financial Fraud Action UK*). As criminals' methods grow ever more sophisticated, *ombudsman focus* brings together expert perspectives on scams and how to stop them.



Rebecca Langford

Rebecca Langford, policy lead for older people at Money Advice Service



“We need to work together to make sure that everyone has the financial capability needed to protect themselves”

In October 2015 the Money Advice Service carried out research which found that more than six in ten people had received a suspicious phone call during a 12 month period. And the Financial Ombudsman Service’s review of complaints about phone fraud found that eight in ten victims were aged over 55.

Scammers are clever and will often exploit the latest technology to impersonate genuine organisations, meaning fraudsters are harder than ever to recognise.

We need to work together to make sure that everyone has the financial capability – the ability, mindset and connection to advice and financial services – needed to protect themselves.

A core element of the UK Financial Capability Strategy is to help people access information and services when they need them. This can be facilitated by bringing organisations together from across sectors so we have a common understanding of the issues, what we want to achieve and how we will get

there. Identifying which initiatives are the most impactful is an essential part of this. That way we can start to improve financial capability.

Unfortunately there is currently very little UK-based impact evaluation of scam awareness programmes.

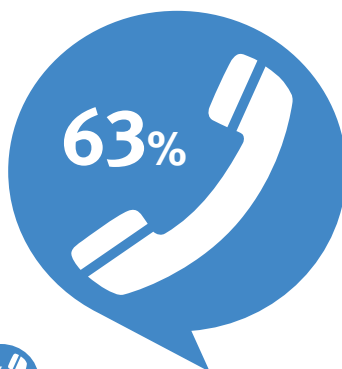
► This means we don't have enough evidence to determine what works best to engage with people about scams to help them protect their finances. With this in mind, we have examined a number of schemes from outside the UK which have been designed to prevent people becoming victims of fraud.

The Daily Money Management programme in the US and the MoneyMinded programme across Australia and the South Pacific are good examples of this. They suggest that maintaining social networks and coordinating different agencies can all help safeguard people against scams.

We will shortly be publishing an evidence review which will provide more detail on 'what works' to improve older people's financial capability, and improving awareness of fraud is part of this. We now need to work collaboratively with organisations across the UK who are engaging with people about scams to identify learnings which can be used to inform future projects.

Further information about the Financial Capability Strategy can be found at www.fincap.org.uk.

63% of people in the UK received a suspicious call over a 12 month period



7% of the UK population – 3.5 million people – had been victims of phone fraud between 2010 and 2015

survey of 2,014 people by Opinium carried out 29 September – 2 October 2015



Katy
Worobec

Katy Worobec, director of Financial Fraud Action UK

Financial Fraud Action UK's membership includes banks, credit, debit and card issuers, and card payment acquirers in the UK. We provide a forum for our members to work together on non-competitive issues relating to financial fraud. Our primary function is to facilitate collaborative activity between industry participants and with other partners.

Every day, banks work extremely hard to protect their customers from fraud. As well as the security features customers are aware of, such as the use of three-digit card security codes when shopping online or over the phone,

there are also a range of other advanced detection and prevention processes working behind the scenes.

These highly sophisticated security systems stopped £7 in every £10 of fraud from happening last year. But despite the industry's best efforts, financial fraud losses totalled £755 million in 2015, an increase of a quarter on 2014. Fraud losses on UK payment cards totalled £567.5 million and remote banking fraud losses stood at £168.6 million last year.

We are determined to do everything in our power to stamp out fraud. The industry is continually evolving its response to financial fraud and this includes investing in new detection and verification tools, working with government and law enforcement through the Joint Fraud Taskforce, as well as educating customers of the dangers.

As the industry uses increasingly secure systems to protect customers, criminals are turning to scams to trick their victims into handing over their passwords,

PINs, passcodes and even their money. If you are a victim of fraud, where you haven't authorised the transaction, you will get your money back. But where customers are duped into moving money to fraudsters, banks will make decisions on refunds on a case-by-case basis.

Our message is that consumers should be very cautious about giving out personal or financial information, and organisations holding data need to do all they can to protect people's private details.

Your bank or the police will never phone you to ask for your PIN or password, ask you to update personal details via a link in a text message or ask you to transfer money to a new account for fraud reasons. Always consider what you are being asked to do. And if you think you have been a victim of fraud, contact your bank immediately.

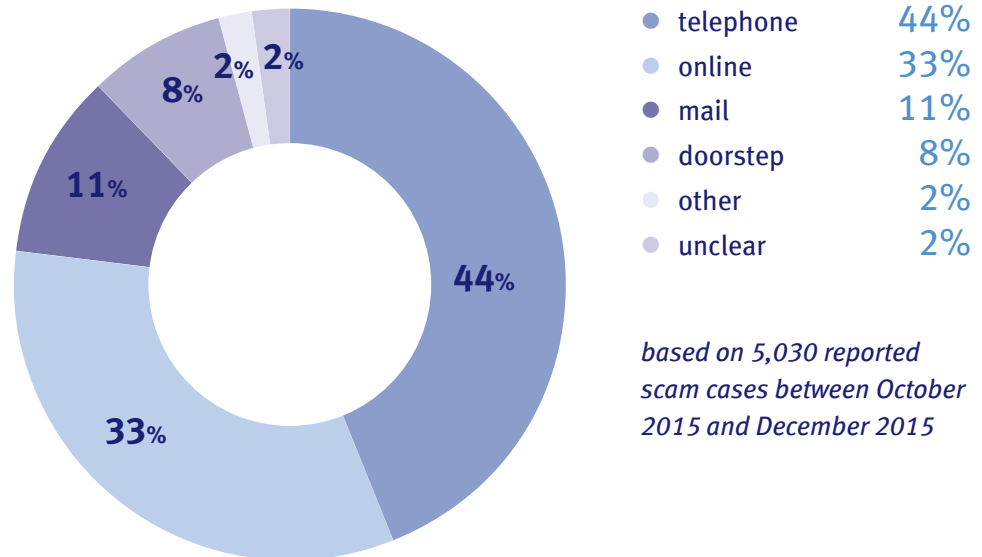


money lost to financial fraud in 2015



Kate Hobson and Nick MacAndrews, Citizens Advice consumer experts give a snapshot of scams reported to Citizens Advice's consumer service.

scams reported to Citizens Advice's consumer service



top five reported scam methods ...

1 **upfront payment fees (29%)** – including requests to pay fees to release compensation payouts or loans, and traders disappearing after payments are made

2 **fake services or invoices (26%)** – including being charged to remove fake computer viruses and fake advertising invoices being sent to small businesses

3 **goods not being received (9%)** – generally involving purchases made through social media or auction websites, where the scammers are private sellers or based abroad

4 **vishing (7%)** – including cold calls asking for credit or debit card details to renew a subscription, or for information about personal debts

5 **subscription traps (7%)** – where people are misled into signing up to subscription services, usually with a free or discounted trial – and scammers then take multiple large payments, often changing their company name

how much money was lost to scams in three months?



£5,926,008

total money reported lost

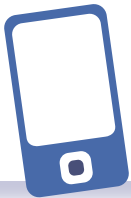
£300,000

most money lost to a single scam

£2,620

average amount lost per victim

average amount lost ...



phone – cold calls about fake computer viruses **£4,496**

online – goods purchased not being received **£1,304**



mail – requests for upfront payments to release lottery winnings **£5,763**

doorstep – requests for upfront payments for building, gardening and maintenance work that was never completed **£2,953**



based on 2,262 cases (45%) where Citizens Advice was able to assess the exact amount of money that had been lost, between October 2015 and December 2015

how did people pay the scammers?

over 50% of cases involved **debit or credit cards** – where victims are more likely to be able to get their money back through chargeback or section 75 claims

based on 2,167 Citizens Advice cases where payment method was known

16% involved **bank transfers** – which are convenient for transferring large sums of money quickly, but can make it difficult to trace where the money has gone

6% involved other **money transfer and voucher payments** which may be convenient for consumers who don't want to give their personal details to make payments, but are untraceable or difficult to trace



*Michael
Ingram*

Michael Ingram, senior ombudsman at the Financial Ombudsman Service

As this ombudsman news highlights, frauds and scams take many different forms. Over the last couple of years we've seen a significant increase in cases where people have been tricked into making payments. The circumstances in which this happens are varied – and, it seems, constantly changing – and can involve payments made online, in branch or over the phone.

In general, you need to be a customer of the business you're complaining about. But in these kinds of fraud cases, we can also look into certain aspects of a complaint about the "receiving" bank the money was sent to.

In most cases though, the money is moved from the receiving bank within minutes – and certainly before anyone realises anything is wrong. Sadly, in nearly all the scams we see, the victim has inadvertently done something that's helped the scammer. For example, they may have given out their password, or given a fraudster remote access to their computer.

We also see cases where a consumer has made a payment themselves – logging in to their online banking and authorising the transaction to the fraudster’s account. Afterwards, it’s easy to see what went wrong. But it’s not always so easy at the time.

From my experience, it seems scammers are successful because the victim is made to believe something’s gone wrong – and things are out of control. And they’re then told they can do something about it, to regain control.

For example, the fraudster might say there’s a security problem with someone’s account – and persuade them to send their money to a “safe” account, which is of course anything but safe. Or the scammer might phone saying they’re from an internet provider, reporting a problem with the service. The victim’s told what they should do to fix the problem – which usually means letting the fraudster access the computer remotely, allowing them access to online banking.

In other cases, the victim buys something online that never arrives, or sells goods and is never paid.

The warning sign is that they’re told to arrange things differently – for example, collecting goods at a “neutral” location instead of posting them, or not using a trusted payment method that provides protection.

Based on the things we’ve seen go wrong, some simple things for consumers to remember are:

- A bank won’t ever ask you to transfer money to a “safe” account.
- A bank doesn’t need a PIN or password to stop a suspicious payment – and they can block a card remotely, without taking it from you.
- An internet service provider won’t ask for access to a computer to fix a problem with a router.

- Online sale and auction sites rely on the parties being able to prove goods have been posted and paid for. If the buyer or seller wants to do something different, it might be a scam.

- A bank or the police would never ask you to get involved in a “sting” operation to help them catch fraudsters.

- A lot of personal information is widely available. Just because someone knows your name, address, date of birth or account numbers doesn’t mean they’re who they say they are.

In some cases, we hear that people are getting phone calls from scammer pretending to be from the Financial Ombudsman Service. The scammers falsely use our name to try to persuade people to reveal details about their personal and financial circumstances.

We never cold-call customers, or email or phone people out of the blue to ask for personal information. And we’ll never ask you for money, or pay compensation to you directly.



Mark
Steward

Mark Steward, director of enforcement and market oversight at the Financial Conduct Authority

One of our priorities at the Financial Conduct Authority is to prevent financial crime, including protecting consumers from unauthorised investment activity and financial fraud.

In 2015 we received over 8,500 reports about potential unauthorised activity. We assess all of these cases and we investigate and take action on as many as we can. This includes taking civil court action to stop activity and freeze assets; insolvency

proceedings; and, for the most serious cases, criminal prosecution. Last year, as a result of our actions, 8 people were sent to jail for a total of 32 years, we froze over £2.7 million, returned nearly £1.9 million to victims and secured injunctions and other orders against unauthorised firms and those behind them. We also issued public warnings about 250 unauthorised firms in order to deter potential investment frauds.

Alongside enforcement action, we also run communications activity to increase consumer awareness of investment fraud and the actions consumers can take to avoid it. Our ScamSmart campaign targets those most at risk of investment fraud. It stresses the importance of rejecting unsolicited calls, checking our Warning List and getting impartial advice before making an investment.

The campaign includes advertising, information on our website, press activity and communications through partners, to build further awareness of the risks posed by investment fraud.

As part of the ScamSmart campaign we created an interactive tool, the FCA Warning List, to help people avoid potential investment fraud. The FCA Warning List is a list of firms and individuals that the FCA knows are operating without its authorisation.

The web tool helps members of the public search this list, find out more about the risks associated with an investment opportunity and find out further steps they can take to avoid investment scams.

It also highlights that if members of the public deal with firms that are not authorised they will not be able to access the Financial Ombudsman Service or the Financial Services Compensation Scheme if things go wrong. Consumers are also encouraged to check the FS Register, which lists authorised firms and individuals we know about.

Only a limited number of investment frauds will fall within our remit, so effective coordination with other agencies and a continued focus on prevention, including better consumer education, is critical to achieving long-term success in this area. We continue to coordinate our efforts across our supervisory, intelligence and enforcement functions in our work on scams and, in particular, those that are targeted at consumers' pensions.

For more information visit www.fca.org.uk/scamsmart.



£1.9m money returned to fraud victims in 2015 as a result of FCA action

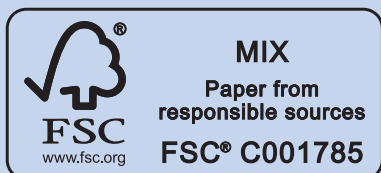
8,500 reports received by FCA in 2015 about potential unauthorised activity

upcoming events ...

smaller business:

<i>meet the ombudsman roadshow</i>	Glasgow	15 September
	Sheffield	19 October

For more information – and to book – go to *news and outreach* on our website.



Printed on Challenger Offset paper made from ECF (Elemental Chlorine-Free) wood pulps, acquired from sustainable forest reserves.

100% of the inks used in *ombudsman news* are vegetable-oil based, 95% of press chemicals are recycled for further use, and on average 99% of waste associated with this publication is recycled.

Q? &A

A few people at our community centre have been having difficulties registering a power of attorney with their bank. How can I help them sort things out? It so often seems to be a question of “computer says no”.

Seeing someone lose mental capacity is likely to be upsetting in itself. And practical barriers to helping them manage their affairs clearly won't make things any easier.

To protect their customers' money, it's only right that businesses will need to have certain procedures and safeguards in place.

But equally, we'd expect businesses to identify and respond to difficult circumstances – and to avoid unreasonable bureaucracy. To help banks and their customers minimise inconvenience and stress, we've shared some tips on our website based on the kinds of problems we see. We've also explained how we can help if things go wrong.

If you'd like to talk through a specific situation, you can phone our free helpline for businesses and people representing consumers on 020 7964 1400.

My son is heading to university in a few weeks – and I'm worried he doesn't know much about finance. Do you have any tips to watch out for based on the complaints you see from young people?

Being in control of your finances for the first time can be a daunting experience – whether it's opening a new account, managing income, or keeping up with bills.

As our latest *annual review* shows, just 1% of the complaints we received last year were brought by people under 25. While that might simply be because younger people haven't yet used many financial products or services, our research suggests they're

also relatively less likely to know about their consumer rights – including the ombudsman. So wise words from people with more experience – such as sharing what we do and how we can help – can be very helpful in case something does go wrong.

Over the past year, we've heard from young people with a range of financial problems – from opening student accounts to insurance claims for stolen phones.

You can find case studies on specific problems we've helped to resolve involving younger people in our September 2015 edition of *ombudsman news*. And we've also shared helpful tips through social media and student publications like the *gap travel guide*.

