

# ombudsman news

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



## fraud and scams: a moving picture



**Caroline Wayman**  
chief ombudsman

It was only relatively recently, in 2015, that we shared our insight into [banking complaints involving phone fraud](#). Back then, it seemed the fact older people were more likely to use landlines meant they were particularly at risk of “no hang up” scams.

### in this issue

**ombudsman  
focus: fraud and  
scams**  
page 3

**fraud and scams  
case studies**  
page 8

**first quarter  
statistics**  
page 14

**Q&A – our new  
case-handling  
system**  
page 17

Today, it's often loopholes in new technologies, rather than in old ones, that fraudsters are using to their advantage. Your first step toward being scammed may be putting your details into an identical, but fake banking website – or responding to a text message that, on the face of it, looks like it's from your bank.

Unlike most other complaints we see, complaints about fraud and scams involve – whether it's accepted or suspected – the actions of a criminal third party. So it's understandable that, in many cases, both the bank and their customer tell us in strong terms that they're not responsible for what's happened.

This makes it harder for us to reach an answer both sides are happy with. But it doesn't mean usual standards don't apply. As our case studies illustrate, we'll expect to see clear evidence that banks have investigated thoroughly – and reflected hard on what more might have been done to protect their customers and their money.

We also often hear from banks that their customers have acted with “gross negligence” – and this means they're not liable for the money their customer has lost. However, gross negligence is more than just being careless or negligent.

And as our case studies show, the evolution of criminals' methods – in particular, their sophisticated use of technology and manipulative “social engineering” – means it's an increasingly difficult case to make.

If there's anything to be salvaged in the wake of fraud and scams, it's what we can learn about how they happened and what needs to change. In this edition, alongside our lead ombudsman Pat Hurley, the Payment Systems Regulator's Hannah Nixon gives an update on regulatory action – including developments in the area of “authorised push payment” fraud, where the FCA is [currently consulting](#) on giving us more powers to help. Fraud expert Richard Emery gives his view on what needs to be done

to stop more people losing more money – and UK Finance's Katy Worobec outlines the industry's response.

The insight we share into what we're seeing – including through *ombudsman news* – is an important part of our work to help prevent complaints arising in the first place. That's especially important for issues such as fraud and scams, where there's high potential for vulnerability and harm.

And in the same way as we want people to learn from our experience, I'm grateful for the insight Richard Lloyd's independent review of our service, published in July, has given us into how we can do things better ourselves. We'll report on the action we've taken in response to his recommendations before the end of the year.

Caroline



*... If there's anything to be salvaged in the wake of fraud and scams, it's what we can learn about how they happened and what needs to change ...*

 @financialombuds  [financial-ombudsman.org.uk](https://financial-ombudsman.org.uk)

 get in touch or subscribe

# ombudsman focus: fraud and scams

According to the [latest data](#) from UK Finance, banks and card companies prevented nearly £1.5 billion from being lost to fraud in 2017. However, more than £730 million was still lost – with “authorised push payment” (APP) fraud, where people unwittingly act on fraudsters’ instructions and carry out the transactions themselves, accounting for a further £236 million of stolen payments.

We asked lead ombudsman Pat Hurley, the Payment Systems Regulator’s Hannah Nixon, independent fraud expert Richard Emery and UK Finance’s Katy Worobec for their perspectives on scams and fraud – and what more needs to be done to prevent them.



**Pat Hurley**  
lead ombudsman and director of casework

The rapid evolution of technology means people are able to engage with financial services in ways that they couldn’t have imagined just a few years ago. And that’s a direction of travel which is only likely to continue. We live in a world now where new technology emerges and is adopted within months, versus the years it took previously. Consumer behaviour and expectations are of course changing in line with this.

Unfortunately, this can provide a fertile ground for scammers who are always moving with the times too. While people may be wiser to emails

from strangers offering unexpected windfalls, today’s scammers are far more sophisticated. This sophistication often manifests itself through a combination of a manipulation of these technological advances and, crucially, social engineering – in other words, manipulating people. The challenge for the financial services sector, its regulators and us at the ombudsman, when we’re deciding what’s fair and reasonable, is to make sure our thinking and our ways of working reflect what’s essentially an ever-changing state of play.

The fact is that scams can be very convincing – for example, using fake websites that look identical to banks’ online systems, or text messages that to all intents and purposes look like they’re from someone’s bank, even joining the message thread of a conversation people had been having with their actual bank. Fraudsters often know the bank’s fraud processes too – playing on the emotions of their targets, who are panicked into thinking their money is at risk right now and perhaps less likely to think clearly as a result.

It's understandable that, in many cases, neither a bank nor their customer feel they've done anything wrong. People who've fallen victim to scams will often tell us they felt they had no option but to do what they were told by the scammers. At the same time, banks often tell us they believe their customers have been "grossly negligent" in handing over personal details to scammers – enabling the scam to occur.

But gross negligence isn't a term to be used lightly. When someone contacts us after losing money to a scam, we'll look to see if they actually authorised the transaction. In assessing this, we'll be trying to "recreate the scene".

If we think it's more likely than not they didn't authorise the transaction, that's when we need to consider whether they were grossly negligent – as part of deciding what's fair and reasonable. And one of the key things we'll think about will be the environment that was created by the fraudster for the consumer – essentially the "spell that was cast".

As financial services change, and scams evolve with it, what's considered grossly negligent behaviour will inevitably change too.

The increasing sophistication of scams means that the bar for gross negligence is high – it's more than just a test of whether someone was careless.

But, like all complaints, if present-day scams have any silver lining, it may be that they can help the financial services sector with its prevention work. And they can also help regulators and the ombudsman service keep in step with what it's fair and reasonable to expect from financial businesses and their customers when it comes to protecting their money.

In fact, if we all continue to learn from today's lessons, then – as consumer understanding and banks' security measures evolve over time – a complaint we uphold today might conceivably not be upheld in a few years' time. Of course, in a perfect world there won't even be fraud to complain about in the first place. But one step at a time.

---

*“one of the key things we'll think about will be the environment that was created by the fraudster”*

---



**Hannah Nixon**  
managing director,  
Payment Systems Regulator

These days financial fraud can happen when we least expect it. Criminals have many different tactics to get hold of our money, and one of them is through authorised push payment (APP) scams – when a fraudster tricks you into transferring money from your bank account to theirs.

We've heard of people in the process of buying a house who have been tricked by fraudsters posing as their conveyancing solicitor, who conned them into transferring and subsequently losing life-changing sums of money. Or people who have paid contractors upfront to carry out work on their homes, only for the "contractor" to disappear with their money.

In the past, the banks didn't have appropriate measures in place to track and stop these scams. There was no reporting of the extent of the problem. There was little by way of making sure consumers were protected, or of getting their money back if they fell prey to a scammer.

We knew that this wasn't good enough and instigated several pieces of work

to help stamp out the problem. We told the banks to accurately record the details of this type of fraud so we could understand the impact properly – and discovered that there were 43,875 reported cases of authorised push payment scams last year, with a total value of £236 million. 88% of the victims were consumers, who lost an average of £2,784. The rest were businesses, who lost on average £24,355 per case.

There are also a number of additional initiatives being developed to combat the problem and provide greater protections. These include guidelines to check the identity of people opening bank accounts to make it harder for fraudsters to open accounts that they use for scams; confirmation of payee, which will allow customers to verify that they are paying the person they want; and improved data sharing, which will mean banks can work together to respond to scams faster and more effectively.

We also tasked the industry to work with consumer representative groups to produce a code that the industry must adhere to when people report scams.

This will give everybody greater protection against this type of fraud – and victims a much better chance of being reimbursed.

We're making good progress and have worked closely with the Financial Ombudsman Service on this important piece of work. In a couple of months the Ombudsman will be able to take this code into account as a relevant consideration when determining new consumer complaints about APP scams. From September 2018 the code will be publicly consulted on, to be refined in early 2019. We know that fraud is an ever-changing beast and we expect the code to continue to evolve to ensure preventative measures are up to date.

Unfortunately, people who have already fallen victim won't benefit from the new protections, but we're committed to making sure that the right measures and incentives are in place to prevent these scams happening in the future. When they do happen, the victims can be confident that they will be given fairer consideration for reimbursement, and that the Ombudsman will be able to hear new complaints under the new code.

*“...we're committed to making sure that the right measures and incentives are in place to prevent these scams happening in the future.”*



**Richard Emery**  
independent forensic fraud investigator,  
4Keys International

*During the last 25 years Richard has served as an expert witness in the civil and criminal justice systems. For the last five years he has focused on the investigation and resolution of payment or bank transaction disputes, primarily involving “gross negligence”, APP scams and fraud.*

## authorised push payment (APP) scams and fraud – past and present

The new code that is being developed by the Payment Systems Regulator and the work that they are doing with the Financial Ombudsman Service are welcome, but this is all about the future. What about the past and the present?

Based on the figures published for 2017 I estimate that in the five years since 2014 over 200,000 individuals, charities and small businesses will have been victims of APP scams and fraud. The majority of these are most likely to have been low-value consumer purchases in response to scam internet offers that turned out to be, quite literally, too good to be true. But this leaves an estimated 50,000 victims who have suffered irrecoverable losses totalling around

£1bn, an average of £20,000 each. Life-changing amounts, but not covered by the new code.

In my view, these high value APP frauds fall into three main categories:

- High-value consumer purchases, where the victim makes a direct payment for an item such as an expensive watch or computer system, but never receives it.
- Expected payment fraud, where the victim is expecting to make a high value payment for goods or services but inadvertently makes the payment to an account controlled by a fraudster, typically in response to an invoice or payment request attached to an email. I believe that this is the most common type of APP fraud and cases that I have seen include a property transaction (£144k), investments (£105k) and paying a genuine builder for work done (£44k).
- Account transfer fraud, where the victim is persuaded that their account is at risk and they need to move their money to a new “safe” account.

Fraudsters are becoming ever more sophisticated, making increased use of highly developed technical skills and social engineering to steal money from our bank accounts. They are exploiting

our reliance on email, the web and the Faster Payments Service (FPS), and the banks are being lamentably slow to respond to the changing landscape.

I look forward to the long overdue proposals for “confirmation of payee” and hope that they will achieve higher levels of payment security without compromising individual privacy.

I value the FPS but fraudsters exploit it. I asked my bank to not release any high-value payments from my account until 24 hours after the payee is created. They declined, saying customers wouldn’t want the delay – but they’ve never actually asked. In any event, they said, FPS rules mean that payments must be made the same day and cannot be delayed. Not so. My bank allows me to “forward date” payments and they comply with FPS rules by making the payment on the forward date. All I’m asking is that they always “forward date” the first high value payment to a new payee by 24 hours.

There is plenty of scope for banks to enhance their security but, in my view, they are unlikely to undertake the necessary investment until they have to take responsibility for more of the losses.

*“Fraudsters are exploiting our reliance on email, the web and the Faster Payments Service”*



**Katy Worobec**  
managing director economic crime,  
UK Finance

## taking the fight to the fraudsters

Fraud is a menace that threatens every part of society and whose perpetrators often target some of the most vulnerable people. It's a threat that requires a response from all sectors, and one that the finance industry is committed to tackling.

Last year, banks' advanced security systems prevented £2 in every £3 of unauthorised fraud. That's £1.4 billion that was stopped from falling into the hands of criminals. Money that otherwise would have gone on to fund illegal activity such as terrorism, drug trafficking and people smuggling.

However, we know there is more to do. While losses due to unauthorised financial fraud fell five per cent last year, they still totalled almost £732 million. And figures collated for the first time on authorised push payment (APP) scams show an additional £236 million was stolen that way in 2017.

That's why the industry has combined forces with the government and the police through the Joint Fraud Taskforce to deter and disrupt the criminals responsible. At the same time, UK Finance is leading the development of

a comprehensive set of initiatives to tackle fraud and scams.

We have established new best practice standards for responding to APP scam claims, so that customers get the help they need. Since they were launched at the start of the year, these standards are already in place across over 80 per cent of the market.

We are hosting the government-led programme to reform the system of economic crime information sharing, known in the industry as Suspicious Activity Reports, so that it meets the needs of crime agencies, regulators, consumers and businesses. And we are working with the Information Commissioner's Office to establish guidance on how data about APP scams can be shared between our members, so they can better protect their customers.

We have developed initiatives such as the Banking Protocol – a ground-breaking rapid response scheme through which branch staff can alert the police and Trading Standards to suspected frauds taking place. The system is now in place across the entire UK and in its first year prevented £25 million in fraud and led to 197 arrests.

The industry also fully sponsors a specialist police unit, the Dedicated Card and Payment Crime Unit, which targets the organised criminal gangs behind these crimes. Last year, the unit prevented almost £30m in fraud and secured 89 convictions.

As the cases often highlighted in Ombudsman News show, criminals are increasingly targeting customers directly using sophisticated techniques, known as social engineering, to trick people into parting with their data or cash.

So it's vital that we also help customers protect themselves. Through our Take Five to Stop Fraud campaign we are equipping people with the knowledge they need to spot the scams and give them the confidence to challenge any out-of-the-blue requests for their personal and financial details or to transfer money.

Sadly, there is no silver bullet in the fight against fraud. But working together and with partners, the finance industry is growing an ever-strengthening arsenal, and this is a battle that we are steadfast in our resolve to win.

*“...working together and with partners, the finance industry is growing an ever-strengthening arsenal”*

# fraud and scams: case studies

In the last financial year, we saw more than 8,000 cases involving people who'd complained to their banks about fraud and scams – in circumstances ranging from disputed card transactions and cash machine withdrawals, to online banking fraud and identity theft.

These case studies illustrate the range of disputes we're called into – which typically arise when a bank has refused to cover the money their customer is saying they've lost. This is generally either because the bank believes their customer acted fraudulently, or because they believe their customer acted with "gross negligence". This reflects the position outlined in the *Payment Services Regulations 2017*, which says a customer (or "payee") is liable for losses if either of these conditions apply. This is something we take into account when we're deciding what's fair and reasonable in all the circumstances.

To decide whether someone authorised what they're saying is a fraudulent transaction, we'll look carefully at the sequence of events leading up to it. But often everyone accepts that the customer didn't actually make the payment – and the dispute instead centres on whether they acted in a "grossly negligent" way.

Demonstrating that a customer acted with gross negligence is a very high bar for a business to meet. As the FCA said in *Payment Services and Electronic Money – Our Approach*:

*"...we interpret "gross negligence" to be a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness."  
(p122)*

Our ombudsman focus highlights the increasing sophistication of criminals' methods. And the fact people are often manipulated into thinking their money's at risk is something we'll think carefully about before deciding whether someone's acted in a way that goes beyond what might be described as careless.

---

*"...often everyone accepts that the customer didn't actually make the payment – and the dispute instead centres on whether they acted in a "grossly negligent" way..."*

---

## 145/1 “Is replying to a text message that I thought was from my bank really “grossly negligent?”

Brian contacted us after his bank refused to refund him money that was stolen from his account in a text message scam.

He explained it had all begun when he'd received a message that he'd thought was from his bank – but that he'd later found out was a “smishing” or SMS scam. His bank was saying that, because he'd given out his security details and passcodes, he'd been “grossly negligent” – and they wouldn't refund the £7,000 he'd transferred unwittingly to the fraudsters.

Brian said everything was so convincing that he couldn't have known he was being scammed. So he didn't think the bank's response was fair – and asked us for our view.

### how we helped

We asked Brian for more information about what had happened to him. He explained he'd received a text message from a number he'd thought to be his bank. In fact, it had gone into the same chain of messages on his phone as genuine messages he'd previously received from the bank.

Brian said the text message had warned of a fraudulent payment and asked him to

phone his bank immediately on the number in the text. He'd done so and spoken to someone who, at the time, he thought worked at his bank. They'd said he would receive a code by text, which he'd need to give to them so they could stop the fraudulent payment leaving his account.

Brian explained that the information he'd been asked to give during the call was just like what he'd been asked for when he'd phoned his bank in the past. So he hadn't realised he was actually talking to fraudsters. And when the code arrived, he'd given it straight to them.

It seemed the payment had then triggered the bank's fraud systems – and another code was sent to him by text. He'd given the fraudsters this code, too – and they'd used it to authorise a payment out of his account. Within minutes, the fraudsters had taken £7,000.

We asked the bank for their view. They told us it was Brian's obligation to take reasonable steps to keep the personalised security features of his account safe. They also told us they emailed their customers warnings about this type of scam – and they thought Brian should have read these.

First, we considered whether Brian had authorised the transactions. We concluded that he hadn't – it had been the fraudsters with the information they'd obtained. We then considered what Brian had said about the initial text message he'd received and the similarity between the security questions asked by his bank and the information he was asked for during the scam. As the scammers appeared to be aware of the bank's fraud and security procedures, including the fact that security codes were sent out by text, we thought Brian's account of what had happened was plausible.

This was clearly a sophisticated fraud. And in light of the worrying and time-sensitive situation Brian had believed he was in – and the way the fraudsters had gained his trust – we thought his actions had been reasonable. We didn't agree with the bank that he'd been grossly negligent – and the fact they'd sent him a general email about scams didn't change our view.

We told the bank to put things right by reimbursing the £7,000 payment to Brian's account.

## 145/2 “Fraudsters took control of my phone and my bank account – why am I being held responsible?”

Mia contacted us after fraudsters stole several thousand pounds from her account.

She'd been told by her bank that she'd put her security details into a fake website. And she'd been told by her mobile phone provider that she'd been a victim of a “SIM swap”. The same fraudsters had apparently been behind both these scams – and had managed to log into her online banking and authorise the payment.

Mia told us her bank were saying she'd been “grossly negligent” in putting her details into the fake website – and were refusing to refund the money she'd lost. Mia didn't think this was fair and asked for our help.

### how we helped

We asked Mia to explain in more detail what had happened. She said she'd noticed the money was missing shortly after having trouble with online banking. She said she hadn't been able to log on, despite being sure she was using the correct details and passwords. The next day, checking her balance at a cash machine, she'd noticed the money was missing from her bank account.

Mia explained she'd had trouble with her mobile phone at the same time. From speaking to her phone provider, she'd discovered fraudsters had also targeted her mobile account. Pretending to be her, they'd managed to get a new SIM card sent out. She now knew these must have been the same fraudsters behind the fake banking website. So when Mia's bank had sent a passcode to her number to authorise the payment, it had been the fraudsters – logged into her online banking – who'd received the code.

Mia's bank said that the fraudsters must have had her security information to make the transfer.

They said Mia had put her details into a fake website designed to look like their own, which had come up near the top of a search engine result. Mia would have thought she was having trouble logging on to her online banking – but actually the fraudsters were collecting the details she was typing in.

The bank showed us images of the scam website they thought Mia had used. In our view, this was almost identical to the bank's own website.

The bank accepted that Mia hadn't authorised the payment from her account. They recognised that, because of the SIM swap, the fraudsters had taken control of Mia's phone and account – so it hadn't been Mia who'd received the passcode. Without this passcode, the login information wouldn't have been enough for the payments to be authorised from Mia's account. And it wasn't Mia's fault that a SIM card had been issued to fraudsters in the first place.

All in all, we didn't agree that Mia had been grossly negligent. So we said the bank should refund the money that was taken as part of the scam.

## 145/3 “The bank says my debit card was used to take money out of my account, but no one uses the card except me.”

Jas contacted us after getting into a dispute with her bank over cash withdrawals she said she didn’t recognise.

She explained she’d noticed several large withdrawals on her monthly statement – and had called her bank to report them as fraudulent. But because she hadn’t been able to explain how they’d happened, the bank had said she must have made them herself or given someone her PIN.

Frustrated that the bank wouldn’t give her money back, Jas wanted us to step in.

### how we helped

Jas told us she never withdrew that much cash in one go – and she hadn’t been at a cash point at the time the transactions happened. She said she couldn’t afford to lose that much money, which was a significant chunk of her monthly pension. She said she’d changed her PIN a few years ago from the one she was issued with, and hadn’t ever told it to anyone.

Jas also said she’d been to the police and tried to get CCTV footage of the cash point, which she thought would prove she hadn’t made the withdrawals.

But the bank had initially directed her to the wrong footage – and by the time they’d realised their mistake, the correct footage had been deleted.

We explained to Jas that CCTV footage can sometimes be an important piece of evidence – and that it should form part of a business’s investigation when it’s available. But we also explained that isn’t always helpful in resolving disputes like hers – as it can sometimes be unclear and so not take us any further forward in understanding what’s happened. We told Jas that because the CCTV footage wasn’t available, we’d look closely at the bank’s records of her transaction history – and weigh these up against everything she’d said.

The bank provided evidence to show Jas’s genuine card had been used for the withdrawals. They’d been made 30 miles from Jas’s house, at separate cashpoints a mile or so apart – just before and just after midnight.

Looking at the pattern of spending on Jas’s account, it seemed she’d made smaller cash withdrawals – which she said she recognised – after the transactions she was disputing. So the card would have had to be

removed and replaced from Jas’s possession.

However, having considered the relevant rules and regulations – in particular, the Payment Service Regulations 2017 – we didn’t think the available evidence was enough to suggest Jas had authorised the transactions. And it was more likely than not that someone else had made the transactions using her card.

We considered what Jas had told us about where she kept her card, and about how no one else knew her PIN. We found her account of what had happened, including what she’d said to the police, to be consistent and plausible. And taking everything into account, we didn’t think the bank had shown she’d been grossly negligent with either of these things.

We recognised that there was a limited number of people that could have made the transactions. But on balance, we didn’t think it was more likely than not that Jas had made or authorised the transactions – or that she’d been grossly negligent. So we told the bank to refund the two disputed transactions.

---

## 145/4 “How can I be responsible for money being taken when I didn’t receive my debit card or my PIN for my new bank

---

Sam contacted us after his bank told him he was making a false claim for disputed transactions.

He explained that, shortly after opening a new bank account, he’d called his bank because he hadn’t received his card or PIN. But the bank had said the card and PIN had already been used for a number of cash withdrawals during the week, using up most of the money in the account.

Sam said he’d told the bank he hadn’t taken the money out himself. But the bank didn’t agree – and their fraud department had told Sam they were closing his account. Left without his money, Sam asked us to help him get it back.

---

## how we helped

---

Sam told us he’d recently started at university, and his parents had given him cash for his accommodation costs and spending money. He explained that after paying his rent, he’d put the rest of the money into the newly-opened account. He said he’d been told his new card and PIN would be sent to him in the post.

Sam told us he’d waited about a week before calling the bank to ask why his card and PIN hadn’t arrived yet. And it seemed that it was during this time that his money had been taken.

The bank said the card and PIN were sent separately to the address Sam had provided. They thought it was unlikely that someone other than Sam had intercepted both pieces of post.

Sam sent us photos of the communal post box in the reception area of his block of flats, which showed post was just left on open shelves. So anyone who had access to the reception area could also have had access to everyone’s post.

The bank told us a further transaction had been attempted and declined two days after Sam had called about the unauthorised

transactions. But from the bank’s records, it didn’t seem their fraud team had actually investigated this transaction – and established whether Sam or someone else had made it – before they’d decided to close Sam’s account.

Taking everything into account, we didn’t think the bank had treated Sam fairly. They couldn’t show on balance that Sam had authorised the withdrawals, or explain why the transaction made after the card was cancelled hadn’t been looked into. So we told them to refund the payments back to Sam.

## 145/5 “My bank says I paid €1,400 for champagne but I only had two G&Ts”

Mel got in touch with us after his bank reinstated a disputed bank transaction for drinks he bought on holiday while he was in what he called a “gentleman’s club”.

He told us he’d ordered two gin and tonics, which he thought had cost €14. But when he’d checked his account the next day, he noticed he had been charged over €1,400.

Mel said he’d contacted his bank – but they’d said they were satisfied the transaction was genuine and wouldn’t return the money.

## how we helped

We asked Mel for his bank statements so we could look at the transaction, along with others he’d made on the same trip. He told us he’d only bought two drinks while at the club, despite being there for several hours.

When we looked at the statements, we found this wasn’t consistent with Mel’s spending at other clubs on the same day, where he’d regularly been spending a considerable amount of money on drinks. Mel told us other people in the group had been buying him drinks, but didn’t have anything to back this up.

We looked at the bank’s records. We saw they’d raised a chargeback as soon as Mel had told them about the incorrect payment. They’d put the money back in his account while they were investigating the transaction with the club. But when the club had provided evidence of the chip and pin transaction, including the sale receipt, the bank had given the money back to the club from Mel’s account at the conclusion of the chargeback process.

Mel didn’t deny that he had used his card and pin to buy drinks at the club. But he was adamant that he had only authorised a payment

of €14 for the drinks he’d bought.

We looked at the receipt the club had provided and saw the order was actually for two bottles of champagne, costing €700 each.

There was no evidence to clarify what the club’s payment terminal had shown when Mel entered his PIN. But looking at all the evidence, we thought it was more likely than not that, if he’d checked the terminal, it would have shown €1,400 – and that he had, at the time, meant to make a payment for that amount. By using his card and entering his PIN, Mel had authorised the transaction – like the other similar transactions he’d made that same night.

We can’t, of course, always know for sure what happened in cases like Mel’s. However, on balance, we thought the bank had done what they should while they were investigating the facts behind the disputed transaction. And we thought it was more likely than not, based on the evidence we’d seen, that Mel had bought the more expensive drinks. So we explained we wouldn’t tell the bank to give him a refund.

# first quarter statistics

## a snapshot of complaints in the first quarter of 2018/2019

Each quarter we publish updates about the financial products and services people have contacted us about. We include the number of enquiries and new complaints we've received, the number of complaints referred for an ombudsman's final decision, and the proportion of complaints we've resolved in consumers' favour.

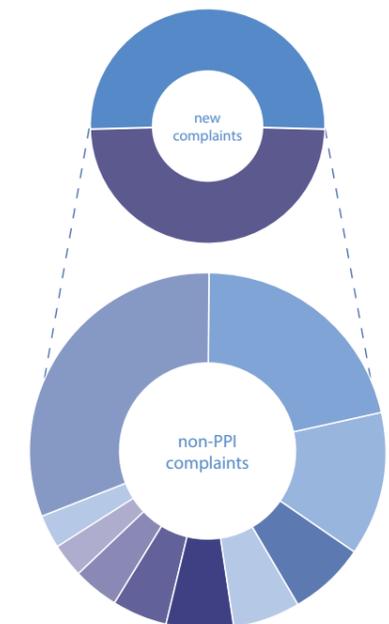
In this issue we show the new complaints we received during April, May and June 2018 – and for comparison, the complaints we received during the same period last year, and during the whole of 2017/2018.

In the first quarter of 2018/2019:

- We received 183,199 enquiries and 107, 827 new complaints – with 11, 371 complaints passed to an ombudsman for a final decision. On average, we upheld 35% of the complaints we resolved.
- PPI remained the most complained-about financial product, with 55,223 new complaints. Payday loans were the second most complained-about product, with 10,979 new complaints.

## the financial products that consumers complained about most to the ombudsman in the first quarter of 2018/2019

- payment protection insurance (PPI) 54%
- complaints about other products 46%
- payday loans 21%
- current accounts 13%
- packaged bank accounts 7%
- car and motorcycle insurance 6%
- credit card accounts 6%
- house mortgages 5%
- hire purchase 4%
- overdrafts and loans 3%
- buildings insurance 3%
- other products 31%



	... in Q1 2018/2019 April 2018 – June 2018				... in Q1 2017/2018 April 2017 – June 2017				... in the whole of 2017/2018 April 2017 – March 2018			
	enquiries received	new cases	ombudsman	% of cases upheld	enquiries received	new cases	ombudsman	% of cases upheld	enquiries received	new cases	ombudsman	% of cases upheld
payment protection insurance	75,966	55,223	4,964	35%	57,186	42,401	1,675	40%	283,623	186,417	13,605	36%
payday loans	14,799	10,979	570	56%	4,384	3,126	564	68%	25,263	17,256	2,080	61%
current accounts	10,354	6,912	621	34%	7,772	5,229	684	27%	32,622	20,217	2,731	26%
packaged bank accounts	5,787	3,520	221	11%	5,269	3,097	219	13%	22,223	11,674	907	11%
car and motorcycle insurance	6,071	3,389	531	30%	6,435	3,137	537	29%	25,411	11,887	1,982	28%
credit card accounts	4,437	3,083	362	35%	3,712	2,640	384	30%	16,753	10,563	1,627	28%
house mortgages	3,456	2,628	401	27%	3,118	2,309	586	24%	13,438	8,888	2,103	23%
hire purchase	2,817	2,031	311	42%	1,944	1,334	255	36%	8,983	5,805	1,172	35%
overdrafts and loans	2,608	1,817	302	25%	2,385	1,589	268	31%	11,020	6,909	1,101	28%
buildings insurance	2,187	1,695	327	39%	1,832	1,261	297	32%	7,503	4,726	1,144	34%
“point of sale” loans	1,424	1,129	90	44%	1,250	1,009	96	32%	5,383	3,613	352	33%
self-invested personal pensions (SIPPs)	1,107	922	137	59%	678	521	181	50%	3,215	2,051	591	52%

first quarter statistics  
continued

	... in Q1 2018/2019 April 2018 – June 2018				... in Q1 2017/2018 April 2017 – June 2017				... in the whole of 2017/2018 April 2017 – March 2018			
	enquiries received	new cases	ombudsman	% of cases upheld	enquiries received	new cases	ombudsman	% of cases upheld	enquiries received	new cases	ombudsman	% of cases upheld
home emergency cover	1,124	869	140	48%	722	568	113	45%	3,448	1,999	415	46%
travel insurance	1,167	798	147	37%	1,082	763	148	39%	5,120	3,165	671	36%
catalogue shopping	951	679	68	45%	882	556	62	51%	3,992	2,191	225	45%
term assurance	607	568	90	18%	591	483	101	16%	3,015	1,977	344	14%
hiring / leasing / renting	826	547	73	40%	548	328	47	30%	2,611	1,587	248	31%
debit and cash cards	705	480	50	34%	708	456	70	26%	2,979	1,844	332	26%
deposit and savings accounts	639	464	74	28%	667	460	67	30%	2,713	1,706	310	29%
contents insurance	655	448	122	25%	650	439	89	27%	2,757	1,743	414	27%
personal pensions	868	436	80	31%	839	438	127	26%	3,118	1,468	397	28%
pet and livestock insurance	566	422	46	29%	616	408	82	25%	2,507	1,544	310	27%
investment ISAs	473	418	77	45%	316	266	66	33%	1,540	1,059	262	35%
whole-of-life policies	566	414	71	19%	457	349	81	20%	2,130	1,304	280	16%
electronic money	896	368	40	26%	861	290	41	32%	3,742	1,155	163	32%
private medical and dental insurance	406	364	69	20%	341	282	63	24%	1,620	1,115	269	24%
inter-bank transfers	593	363	33	28%	473	322	47	27%	2,150	1,222	183	27%
credit reference agency	534	347	22	36%	449	217	15	33%	2,242	1,060	96	32%
debt collecting	779	314	30	34%	752	263	39	28%	3,213	998	177	29%
home credit	337	308	22	40%	82	68	15	20%	1,223	808	102	34%
mortgage endowments	489	283	48	24%	476	258	49	15%	2,213	1,078	218	14%
income protection	338	276	52	23%	268	205	48	18%	1,300	865	195	20%
share dealings	322	273	55	45%	267	148	64	30%	1,449	763	209	32%
critical illness insurance	312	255	67	15%	266	204	49	20%	1,278	861	197	19%
specialist insurance	365	248	42	51%	460	419	45	31%	1,581	1,076	158	33%
warranties	420	237	44	52%	431	260	56	44%	1,884	919	178	44%
instalment loans	289	224	69	60%	221	172	68	50%	1,554	1,122	393	58%
roadside assistance	368	219	44	34%	235	162	28	34%	1,220	712	120	36%
mobile phone insurance	403	217	37	32%	454	279	32	37%	1,829	977	110	39%
portfolio management	230	198	76	41%	265	227	87	40%	1,112	815	364	37%
occupational pension transfers and opt outs	180	184	52	32%	160	124	63	29%	817	553	240	30%
legal expenses insurance	203	173	59	28%	215	172	65	31%	952	660	239	30%
cash ISA - Individual Savings Account	228	172	19	25%	203	133	21	24%	718	484	89	29%
secured loans	224	165	36	24%	317	236	56	21%	1,174	781	187	25%
direct debits and standing orders	291	162	18	35%	268	135	29	33%	1,079	501	79	31%
commercial vehicle insurance	230	158	33	46%	212	109	27	27%	1,002	523	113	32%
annuities	146	148	29	19%	264	227	46	14%	940	744	188	16%
merchant acquiring	225	141	13	35%	189	115	16	23%	889	510	67	31%
store cards	204	137	17	37%	184	114	21	35%	889	508	67	37%
cheques and drafts	191	135	17	44%	189	122	14	36%	740	447	85	35%
conditional sale	130	118	31	46%	144	111	31	34%	731	533	151	38%
personal accident insurance	145	95	18	15%	173	105	13	17%	630	410	76	23%

first quarter statistics  
continued

	... in Q1 2018/2019 April 2018 – June 2018				... in Q1 2017/2018 April 2017 – June 2017				... in the whole of 2017/2018 April 2017 – March 2018			
	enquiries received	new cases	ombudsman	% of cases upheld	enquiries received	new cases	ombudsman	% of cases upheld	enquiries received	new cases	ombudsman	% of cases upheld
commercial property insurance	94	88	20	38%	86	71	33	35%	422	269	113	30%
building warranties	97	87	24	33%	119	89	28	29%	472	290	106	32%
unit-linked investment bonds	56	82	33	41%	86	73	32	39%	388	306	117	31%
card protection insurance	132	81	4	25%	178	94	7	34%	751	347	24	26%
guarantor loans	107	70	12	34%	63	34	11	20%	368	210	48	22%
guaranteed asset protection (“gap” insurance)	103	68	9	20%	92	61	7	22%	421	209	36	24%
derivatives	49	67	19	11%	50	49	39	28%	290	183	94	19%
“with-profits” bonds	57	55	20	25%	73	52	19	19%	266	188	75	23%
income drawdowns	48	55	8	47%	46	45	15	35%	202	169	54	36%
business protection insurance	58	53	10	25%	71	54	12	23%	314	189	53	25%
money remittance	107	49	9	31%	170	101	8	27%	610	305	50	29%
spread betting	51	44	27	13%	66	50	37	15%	289	179	89	22%
endowment savings plans	59	43	18	38%	86	62	21	30%	380	263	80	25%
investment trusts	-	-	-	-	113	61	8	44%	364	199	48	38%
credit broking	-	-	-	-	86	50	14	33%	403	202	49	25%
debt adjusting	-	-	-	-	89	44	9	26%	315	135	26	28%
capital protected structured products	-	-	-	-	22	30	14	19%	169	137	59	29%
foreign currency	-	-	-	-	-	-	-	-	308	132	20	19%
unit trusts	-	-	-	-	-	-	-	-	175	121	38	34%
caravan insurance	-	-	-	-	-	-	-	-	213	119	32	28%
free standing additional voluntary contributions (FSAVC)	-	-	-	-	-	-	-	-	170	116	33	27%
logbook loans	-	-	-	-	-	-	-	-	178	113	32	37%
open-ended investment companies (OEICs)	-	-	-	-	-	-	-	-	153	110	45	18%
premium bonds	-	-	-	-	-	-	-	-	206	98	15	21%
safe custody	-	-	-	-	-	-	-	-	132	98	21	45%
savings certificates/bonds	-	-	-	-	-	-	-	-	180	99	17	23%
state earnings-related pension (SERPs)	-	-	-	-	-	-	-	-	148	92	16	8%
personal equity plans (PEP)	-	-	-	-	-	-	-	-	112	92	33	23%
debt counselling	-	-	-	-	-	-	-	-	205	88	15	21%
executorships/trusteeships	-	-	-	-	-	-	-	-	97	56	14	40%
pawnbroking	-	-	-	-	-	-	-	-	93	55	12	49%
banker’s reference	-	-	-	-	-	-	-	-	109	47	5	37%
interest rate hedge	-	-	-	-	-	-	-	-	53	40	41	21%
children’s savings plans	-	-	-	-	-	-	-	-	66	33	10	20%
non-structured periodically guaranteed fund	-	-	-	-	-	-	-	-	31	30	11	24%
<b>sub total</b>	<b>150,656</b>	<b>106,995</b>	<b>11,180</b>	<b>35%</b>	<b>114,358</b>	<b>79,666</b>	<b>8,261</b>	<b>35%</b>	<b>540,591</b>	<b>339,112</b>	<b>39,847</b>	<b>35%</b>
<b>other products and services</b>	<b>32,543</b>	<b>832</b>	<b>191</b>	<b>34%</b>	<b>21,421</b>	<b>568</b>	<b>153</b>	<b>30%</b>	<b>72,276</b>	<b>855</b>	<b>173</b>	<b>30%</b>
<b>total</b>	<b>183,199</b>	<b>107,827</b>	<b>11,371</b>	<b>35%</b>	<b>135,779</b>	<b>80,234</b>	<b>8,414</b>	<b>35%</b>	<b>612,867</b>	<b>339,967</b>	<b>40,020</b>	<b>34%</b>



## I read in your *annual review* that you're getting a new case-handling system. Will that have any impact on how my business needs to engage with the ombudsman service?

Our new case-handling system is part of our wider work to improve our digital capability – helping us make sure we're working as efficiently as possible, and in a way that's personal and convenient for anyone who uses our service. As well as the new system, in the coming months we'll also be launching our online portals, reviewing how we record complaints, and improving our online content.

We plan to launch our new case-handling system in October 2018. While most of the changes we're making won't be visible to anyone outside the ombudsman service, there may be some things you need to consider.

---

### what changes will I see?

Our case reference numbers are changing to a new format. The reference will start with the prefix "PNX" – because our new system is called Phoenix. Then there will be five numbers, ending with a four digit suffix made up of a combination of letters and numbers. Each part is separated by a hyphen, so you'll end up with something like PNX-12345-A1B2.

This won't affect all cases immediately. And if a case is already with us, we'll continue to use the existing eight-digit reference. So, there'll be a period where you'll see references in both formats.

We're also changing the format of our case handlers' email addresses. The new format will be name.surname@cases.financial-ombudsman.org.uk. These changes will help us handle case-related emails more efficiently. While we're transitioning from our old case handling system to our new one, you may notice that our case handlers will be using both addresses at the same time. It doesn't matter which one you reply to – everything will get to the right place.

---

### is there anything I need to do?

- It's worth checking whether our new case reference numbers will be an issue for any IT systems you use. If you think this might cause you problems, please contact our [technical advice desk](#) as soon as possible.
- From October, if we have an email address on file for the person we're contacting at your business, all correspondence will be sent by email. If you want to continue to receive correspondence by post, please contact our [technical advice desk](#).
- The letters we generate from our system will look different in the future. If you use scanning software that recognises our current letters, please contact our [technical advice desk](#) so we can give you more details.



### is there anything else I need to know?

On 25 May 2018 the General Data Protection Regulation (GDPR) came into force. We've already updated and made some changes to our complaint form in line with GDPR and to ensure a smooth experience for people using our service. Although it's unlikely you'll need to use this form yourself, you

might see it as part of correspondence about complaints. The updated version is available on [our website](#).

If you have any other questions, please email [technical.advice@financial-ombudsman.org.uk](mailto:technical.advice@financial-ombudsman.org.uk).



#### meet us in...

♦ Stirling 13 September 2018

See [our website](#) for more information