complaint

Mr W is unhappy because National Westminster Bank Plc (NatWest) refuses to give him back the money he says a fraudster took from his account. And he says he received poor customer service after he reported the fraud to the bank.

background

In October 2017 Mr W was a victim of a scam. It's not in dispute that what happened was an act of fraud. So I've used the term "fraudster" throughout to refer to the third party involved. Based on the submissions made by both parties I understand the scam occurred in the following way:

Mr W received a call on 29 October 2017 at 18.28 from someone who said he worked for NatWest. Mr W didn't have NatWest's phone number stored on his phone but the call showed up as coming from an "0345" number with a "SMART" caller ID label of "NatWest". The caller/fraudster asked for Mr W by name and then explained:

- the bank had identified that someone had tried to take £120 from Mr W's account;
- the bank needed to cancel Mr W's debit card and online banking access to prevent any further fraud; and
- the bank would send Mr W a code which he needed to tell them in order to cancel the debit card and online banking.

The code came through by text message at 18.31, while Mr W was still on the phone with the fraudster. He says he didn't need to open the actual text because the code popped up at the top of his mobile phone screen. He didn't see any warnings relating to the code and simply read out the six digits. The fraudster said he would arrange for Mr W's card and online banking to be cancelled and ended the call.

Mr W originally said – to NatWest and us – that he didn't give the fraudster any other personal or banking details. When we pressed him on this he said he couldn't completely rule out the possibility that he may have, perhaps, confirmed his address and date of birth.

Mr W already had the mobile banking app on his own phone. And NatWest has explained the process a person must go through in order to set up the app on a second device. It seems likely, given the process NatWest has described, that the fraudster had already downloaded NatWest's mobile banking app to his own mobile handset when he called Mr W. The next step in order to register a second device for mobile banking is to request an activation code by entering a mobile number that is already linked to a NatWest account. The fraudster likely entered Mr W's mobile number and that was what generated the text message Mr W received, containing a six-digit activation code. The fraudster will likely have entered that code into the app he'd already downloaded to his own phone, which allowed him to move onto the next stage of the mobile banking app activation process. The steps necessary to complete activation were as follows:

- Choose, enter and re-enter a passcode of between five and eight digits (this is used to access the app after it's activated).
- Enter Mr W's online banking customer number (which consisted of Mr W's date of birth and four other digits).
- Enter three digits from Mr W's online banking PIN (selected at random by the app)

- Enter three characters from Mr W's online banking password (selected at random by the app).

NatWest's audit trail shows the fraudster completed the registration process and logged onto Mr W's account at 18.32. He had an iPhone whereas Mr W's handset was Android, and this distinction is made clear on the audit trail, so it's easy to see which activity related to which person's phone. The fraudster subsequently completed the following transactions via the mobile banking app:

18.57 £20 transfer to a new payee (account ending 5086), post-dated to 30/10
19.00 £120 "Get Cash" code requested which was subsequently used to withdraw £120 cash from a retailer's cash machine
19.02 £130 PAYM payment to account ending 5086, post-dated to 30/10
19.04 £10 "Get Cash" code requested which was subsequently used to withdraw £10 cash from a retailer's cash machine
20.33 £100 low value payment to account ending 7866, post-dated to 30/10
20.34 £150 low value payment to account ending 7866, post-dated to 30/10
20.36 £530 transferred from Mr W's ISA to his current account, post-dated to 30/10

On 30 October 2017 the fraudster completed the following further transactions:

00.06 £100 low value payment to account ending 7866
00.06 £150 low value payment to account ending 7866
00.07 £250 transferred from Mr W's ISA to his current account

NatWest's audit trail shows Mr W logged onto his mobile banking app on 30 October 2017 between 09.27 and 09.31. He tells us he can't remember exactly what he saw when he logged on but it was probably more transactions than he expected to see. At 09.32 he called NatWest using the same "0345" number from which the call appeared to originate the night before. NatWest has given us a recording of the first part of the call in which Mr W explained the bank had called him the night before and he wanted to speak further with someone about this. NatWest's adviser said she could see Mr W's account was on hold and put him through to the fraud team. NatWest hasn't been able to give us a recording of the second part of the call. So I don't know what Mr W told the bank at that point, for example, about what he'd seen when he logged onto his account just before he called or what had happened during the call the night before.

But NatWest has given us recordings of subsequent calls in which Mr W explained again what had happened and raised a formal complaint when the bank said it wouldn't refund his money.

NatWest's records show it called the bank to which some of Mr W's money was transferred, on 30 October 2017 at 10.54. But the money had already been withdrawn, so the bank wasn't able to reclaim any of this for Mr W. The other transfers went into another NatWest account and it's not clear if the bank checked that account at the same time. Records show that most of the money had been transferred out by the end of 30 October 2017 but it's not clear what time these transactions took place and £37.29 remained as a credit balance at the end of that day. NatWest didn't make any attempts to remove this money.

NatWest refused to refund any of the money the fraudster took from Mr W's accounts because it said he'd given away the mobile banking activation code.

Mr W also complained about the way NatWest had dealt with him after he reported the fraud. He said the bank failed to report the fraud to the police after saying it would do so, he kept being put on hold and transferred around and it was insensitive of the bank's staff to say the fraud was his fault and to tell him to stop calling. NatWest said it had contacted Mr W about his complaint within its usual timescales but the bank accepted it may not have provided an appropriate level of service. So it paid £50 compensation into Mr W's account.

NatWest has also explained:

- The text Mr W was sent with the mobile banking app activation code also said *"Warning: never reveal this code to anyone".*

- The "Get Cash" facility allows a customer to withdraw up to £130 cash each day from their account without their debit card. The "Get Cash" code is requested via the customer's mobile banking app and can be used to withdraw the cash from an ATM owned by NatWest or one other, specified retailer.

- The mobile banking app allows customers to "pay someone new" using just the recipient's sort code and account number without the need to set them up via online banking using their debit card and card reader. Up to five "low value payments" totalling not more than £250 can be made to each recipient each working day.

- The mobile banking app allows payments of up to £250 per day, per recipient to be sent using the PAYM service. Money can be sent to any person in the customer's mobile phone contact list using their mobile number rather than their sort code and account number.

- The mobile banking app can be downloaded and active on two devices at any one time. And the relevant devices are "tracked by mobile number". But they haven't explained how this actually works or what security this tracking provides.

- When Mr W called the bank on 30 October 2017 he was told his account was already blocked. That's correct, but the block wasn't activated in relation to this mobile banking fraud. It arose in relation to a transaction performed using Mr W's debit card and NatWest can't now give us any more details about that. It wasn't followed up at the time because this fraud took priority. And the bank says now it doesn't think the two were related given that this fraud was perpetrated using mobile banking and Mr W hasn't raised any concerns about any debit card transactions. His debit card was cancelled after he reported the mobile banking fraud and there's no suggestion that this wasn't in his possession at that time.

- It has run radio adverts, sponsored UK-wide TV adverts and displayed security information on its website and online banking to help customers spot scams.

my provisional decision

On 27 November 2018 I issued a provisional decision on Mr W's complaint. After considering all of the evidence and arguments presented by both sides, I was minded to conclude that:

- Mr W did not authorise the transactions in question.

- Mr W had not acted with gross negligence.

- NatWest should fairly and reasonably refund the money taken from Mr W, plus interest at the rate he would have received had the money remained in his ISA account.

I have attached a copy of my provisional decision to this final decision – it forms part of this final decision and details in full how and why I reached those conclusions.

after my provisional decision

Mr W said he agreed with my provisional findings and had no further information to add.

NatWest said, in order to bring a prompt close to Mr W's complaint, it accepted the outcome I had proposed for this particular case only.

my findings

I've reconsidered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

As no-one sent any further evidence or arguments for me to consider, I see no reason to depart from the conclusions set out in my provisional decision (as attached) and summarised above.

my final decision

My final decision is that I uphold this complaint and I instruct National Westminster Bank Plc to:

1. Credit Mr W's current account with £780. In making this refund the bank, in accordance with the terms and conditions applicable to Mr W's account, is entitled to withhold up to £50. If it exercises this right, I consider it would be fair and reasonable for it to inform Mr W of its decision to do so.

2. Add interest from the date of the disputed transactions to the date of settlement at the rate Mr W would have received had the money not been moved from his ISA account into his current account and removed by the fraudster. That interest would have been paid gross because the money was in an ISA. But if NatWest thinks it must deduct tax from the interest element of this award, it should provide Mr W with the appropriate tax deduction certificate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 21 January 2019.

Ruth Hersey
ombudsman

COPY OF PROVISIONAL DECISION

complaint

Mr W is unhappy because National Westminster Bank Plc (NatWest) refuses to give him back the money he says a fraudster took from his account. And he says he received poor customer service after he reported the fraud to the bank.

background

In October 2017 Mr W was a victim of a scam. It's not in dispute that what happened was an act of fraud. So I've used the term "fraudster" throughout to refer to the third party involved. Based on the submissions made by both parties I understand the scam occurred in the following way:

Mr W received a call on 29 October 2017 at 18.28 from someone who said he worked for NatWest. Mr W didn't have NatWest's phone number stored on his phone but the call showed up as coming from an "0345" number with a "SMART" caller ID label of "NatWest". The caller/fraudster asked for Mr W by name and then explained:

- the bank had identified that someone had tried to take £120 from Mr W's account;
- the bank needed to cancel Mr W's debit card and online banking access to prevent any further fraud; and
- the bank would send Mr W a code which he needed to tell them in order to cancel the debit card and online banking.

The code came through by text message at 18.31, while Mr W was still on the phone with the fraudster. He says he didn't need to open the actual text because the code popped up at the top of his mobile phone screen. He didn't see any warnings relating to the code and simply read out the six digits. The fraudster said he would arrange for Mr W's card and online banking to be cancelled and ended the call.

Mr W originally said – to NatWest and us – that he didn't give the fraudster any other personal or banking details. When we pressed him on this he said he couldn't completely rule out the possibility that he may have, perhaps, confirmed his address and date of birth.

Mr W already had the mobile banking app on his own phone. And NatWest has explained the process a person must go through in order to set up the app on a second device. It seems likely, given the process NatWest has described, that the fraudster had already downloaded NatWest's mobile banking app to his own mobile handset when he called Mr W. The next step in order to register a second device for mobile banking is to request an activation code by entering a mobile number that is already linked to a NatWest account. The fraudster likely entered Mr W's mobile number and that was what generated the text message Mr W received, containing a six-digit activation code. The fraudster will likely have entered that code into the app he'd already downloaded to his own phone, which allowed him to move onto the next stage of the mobile banking app activation process. The steps necessary to complete activation were as follows:

- Choose, enter and re-enter a passcode of between five and eight digits (this is used to access the app after it's activated).
- Enter Mr W's online banking customer number (which consisted of Mr W's date of birth and four other digits).
- Enter three digits from Mr W's online banking PIN (selected at random by the app)
- Enter three characters from Mr W's online banking password (selected at random by the app).

NatWest's audit trail shows the fraudster completed the registration process and logged onto Mr W's account at 18.32. He had an iPhone whereas Mr W's handset was Android, and this distinction is made clear on the audit trail, so it's easy to see which activity related to which person's phone. The fraudster subsequently completed the following transactions via the mobile banking app:

18.57 £20 transfer to a new payee (account ending 5086), post-dated to 30/10
19.00 £120 "Get Cash" code requested which was subsequently used to withdraw £120 cash from a retailer's cash machine
19.02 £130 PAYM payment to account ending 5086, post-dated to 30/10
19.04 £10 "Get Cash" code requested which was subsequently used to withdraw £10 cash from a retailer's cash machine
20.33 £100 low value payment to account ending 7866, post-dated to 30/10
20.34 £150 low value payment to account ending 7866, post-dated to 30/10
20.36 £530 transferred from Mr W's ISA to his current account, post-dated to 30/10

On 30 October 2017 the fraudster completed the following further transactions:

00.06 £100 low value payment to account ending 7866
00.06 £150 low value payment to account ending 7866
00.07 £250 transferred from Mr W's ISA to his current account

NatWest's audit trail shows Mr W logged onto his mobile banking app on 30 October 2017 between 09.27 and 09.31. He tells us he can't remember exactly what he saw when he logged on but it was probably more transactions than he expected to see. At 09.32 he called NatWest using the same "0345" number from which the call appeared to originate the night before. NatWest has given us a recording of the first part of the call in which Mr W explained the bank had called him the night before and he wanted to speak further with someone about this. NatWest's adviser said she could see Mr W's account was on hold and put him through to the fraud team. NatWest hasn't been able to give us a recording of the second part of the call. So I don't know what Mr W told the bank at that point, for example, about what he'd seen when he logged onto his account just before he called or what had happened during the call the night before.

But NatWest has given us recordings of subsequent calls in which Mr W explained again what had happened and raised a formal complaint when the bank said it wouldn't refund his money.

NatWest's records show it called the bank to which some of Mr W's money was transferred, on 30 October 2017 at 10.54. But the money had already been withdrawn, so the bank wasn't able to reclaim any of this for Mr W. The other transfers went into another NatWest account and it's not clear if the bank checked that account at the same time. Records show that most of the money had been transferred out by the end of 30 October 2017 but it's not clear what time these transactions took place and £37.29 remained as a credit balance at the end of that day. NatWest didn't make any attempts to remove this money.

NatWest refused to refund any of the money the fraudster took from Mr W's accounts because it said he'd given away the mobile banking activation code.

Mr W also complained about the way NatWest had dealt with him after he reported the fraud. He said the bank failed to report the fraud to the police after saying it would do so, he kept being put on hold and transferred around and it was insensitive of the bank's staff to say the fraud was his fault and to tell him to stop calling. NatWest said it had contacted Mr W about his complaint within its usual timescales but the bank accepted it may not have provided an appropriate level of service. So it paid £50 compensation into Mr W's account.

NatWest has also explained:

- The text Mr W was sent with the mobile banking app activation code also said *"Warning: never reveal this code to anyone".*

- The "Get Cash" facility allows a customer to withdraw up to £130 cash each day from their account without their debit card. The "Get Cash" code is requested via the customer's mobile

banking app and can be used to withdraw the cash from an ATM owned by NatWest or one other, specified retailer.

- The mobile banking app allows customers to "pay someone new" using just the recipient's sort code and account number without the need to set them up via online banking using their debit card and card reader. Up to five "low value payments" totalling not more than £250 can be made to each recipient each working day.

- The mobile banking app allows payments of up to £250 per day, per recipient to be sent using the PAYM service. Money can be sent to any person in the customer's mobile phone contact list using their mobile number rather than their sort code and account number.

- The mobile banking app can be downloaded and active on two devices at any one time. And the relevant devices are "tracked by mobile number". But they haven't explained how this actually works or what security this tracking provides.

- When Mr W called the bank on 30 October 2017 he was told his account was already blocked. That's correct, but the block wasn't activated in relation to this mobile banking fraud. It arose in relation to a transaction performed using Mr W's debit card and NatWest can't now give us any more details about that. It wasn't followed up at the time because this fraud took priority. And the bank says now it doesn't think the two were related given that this fraud was perpetrated using mobile banking and Mr W hasn't raised any concerns about any debit card transactions. His debit card was cancelled after he reported the mobile banking fraud and there's no suggestion that this wasn't in his possession at that time.

- It has run radio adverts, sponsored UK-wide TV adverts and displayed security information on its website and online banking to help customers spot scams.

my provisional findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint. When considering what's fair and reasonable, I'm required to take into account: relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.

relevant considerations

NatWest is a Financial Conduct Authority (FCA) regulated firm, and was carrying out regulated activities. As such the FCA's overarching Principles for Businesses apply including the requirement to pay due regard to a customer's interest and treat them fairly (Principle 6).

The transactions from Mr W's account were made in October 2017. So the relevant legislation is that set out in the Payment Services Regulations 2009 (PSR 2009)[1]. I think the following sections of PSR 2009 are of particular relevance here:

"Consent and withdrawal of consent

55.—(1) A payment transaction is to be regarded as having been authorised by the payer for the purposes of this Part only if the payer has given its consent to—

(a) the execution of the payment transaction; …"

[1] The Payment Services Regulations 2009 were replaced in January 2018, which resulted in some regulations now carrying different numbers. All references in this decision to the Payment Services Regulations mean the 2009 regulations.

"Obligations of the payment service user in relation to payment instruments

57.—(1) A payment service user to whom a payment instrument has been issued must—

(a) use the payment instrument in accordance with the terms and conditions governing its issue and use; and
(b) notify the payment service provider in the agreed manner and without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

(2) The payment service user must on receiving a payment instrument take all reasonable steps to keep its personalised security features safe."

"Evidence on authentication and execution of payment transactions

60.—(1) Where a payment service user—

(a) denies having authorised an executed payment transaction; or
(b) claims that a payment transaction has not been correctly executed,

it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the payment service provider's accounts and not affected by a technical breakdown or some other deficiency.

(2) In paragraph (1) "authenticated" means the use of any procedure by which a payment service provider is able to verify the use of a specific payment instrument, including its personalised security features.

(3) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider is not in itself necessarily sufficient to prove either that—

(a) the payment transaction was authorised by the payer; or
(b) the payer acted fraudulently or failed with intent or gross negligence to comply with regulation 57."

"Payment service provider's liability for unauthorised payment transactions

61. Subject to regulations 59 [Notification of unauthorised or incorrectly executed payment transactions] *and 60, where an executed payment transaction was not authorised in accordance with regulation 55, the payment service provider must immediately—*

(a) refund the amount of the unauthorised payment transaction to the payer; and
(b) where applicable, restore the debited payment account to the state it would have been in had the unauthorised payment transaction not taken place."

"Payer's liability for unauthorised payment transaction

62.—(1) Subject to paragraphs (2) …, the payer is liable up to a maximum of £50 for any losses incurred in respect of unauthorised payment transactions arising—

(a) from the use of a lost or stolen payment instrument; or
(b) where the payer has failed to keep the personalised security features of the payment instrument safe, from the misappropriation of the payment instrument.

(2) The payer is liable for all losses incurred in respect of an unauthorised payment transaction where the payer—

(a) has acted fraudulently; or
(b) has with intent or gross negligence failed to comply with regulation 57."

consent

Regulation 55 doesn't elaborate on what constitutes consent beyond saying that it *"must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider".* The payment services directive itself (which the PSR 2009 implement) doesn't explain what consent means here, but says *"In the absence of such consent, a payment transaction shall be considered to be unauthorised."* The FCA's 2013 guidance on the PSR 2009 also said nothing further about what consent means.

So I think it's fair, when considering whether consent was given, to apply the common definition of consent, which is to give permission for something to happen.

gross negligence

Whether a customer has acted with *"gross negligence"* is something that can only be assessed on a case by case basis, taking into account all the circumstances. The term is not defined in PSR 2009 or in the first Payment Services Directive. But recital 72 of the second Payment Services Directive provides as follows:

"In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties…"

Reflecting this, the FCA, in its document setting out its role under the Payment Services Regulations 2017, says:

"… 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."

Although neither of these is directly relevant to this complaint, they're of value as a relevant consideration in the absence of contemporaneous interpretative guidance, and because they inform the meaning of a concept that has been in place for some time (in the Banking Code).

When considering gross negligence in a commercial contract context, Mance J in Red Sea Tankers Ltd v Papachristidis (The "Ardent") [1997] 2 Lloyd's Rep 547, 586 said:

"If the matter is viewed according to purely English principles of construction, … "Gross" negligence is clearly intended to represent something more fundamental than failure to exercise proper skill and/or care constituting negligence… as a matter of ordinary language and general impression, the concept of gross negligence seems to me capable of embracing not only conduct undertaken with actual appreciation of the risks involved, but also serious disregard of or indifference to an obvious risk."

Negligence is often referred to as a failure to exercise reasonable care, but as I have described above gross negligence suggests a lack of care that goes significantly beyond ordinary negligence. So I have to consider whether Mr W's actions fell so far below the standard of a reasonable person that it would be fair to say he failed with gross negligence to keep his personalised security details safe or to comply with the terms and conditions of his account.

the terms and conditions of Mr W's account

The following extracts from the general terms and conditions of Mr W's current account are also relevant to this case. These terms and conditions broadly reflect the provisions contained in the PSR 2009.

2.4 Protecting your account

You must:
*(a) keep your **PIN** (personal identification number) and other security details secret: and*
(b) tell us immediately if you think someone else may know your security details or if you suspect unauthorised use of your account by phoning us on 0345 300 3983 (or +44 131 339 7609 from abroad) or by contacting your local branch.

4.5 Unauthorised or incorrect payments

4.5.1 This Term sets out your and our responsibilities if unauthorised or incorrect payments are made from your account. It does not deal with the effects of misusing of a card, which is covered in the Card Terms.

4.5.2 If you suspect that an unauthorised or incorrect payment has been made from your account, please contact us immediately by phoning us on 0345 788 8444 or contacting your local branch.

4.5.3 If you do not tell us promptly and in any event within 13 months after the date the payment was debited from your account, you will not be entitled to have any error corrected, payment amount refunded or to be compensated for any loss suffered. Otherwise and subject to General Terms 4.5.4 to 4.5.9. an unauthorised or incorrect payment of which you have given notice will be refunded and. where applicable, your account will be restored to its position had the unauthorised or incorrect payment not taken place. We will have no further liability to you in relation to any unauthorised payment. The 13 month time limit does not apply to payments made by cheque or to any other type of payment which has the effect of creating or increasing an overdrawn balance on your account.

4.5.4 You are responsible for the payment and your account will not be refunded where you have acted fraudulently. None of the provisions limiting your liability set out in General Term 4.5.5 to General Term 4.5.7 will apply.

4.5.5. Where you have:
(a) allowed another person to make payments (other than someone that we have agreed may be allowed to use your account): or
(b) failed intentionally or with gross negligence, to keep your security details secret and a credit balance on your account is reduced by the unauthorised payment(s). you will be responsible for all payments made in this way before you tell us that any transactions are unauthorised.

4.5.6 You will not be responsible for any unauthorised payments where:
(a) you have not yet received your security details: or
(b) these have been made by someone who has your security details and has used them without your authority to make a payment where the account holder does not need to be present, such as the purchase of goods or services by telephone, over the internet or mail order.

4.5.7 Unless General Terms 4.5.4 to 4.5.6 above apply, where your security details are lost or stolen, or you do not keep them safe as you are obliged to do under this agreement, you may be responsible for unauthorised transactions, up to a maximum of £50. You will not be

responsible for any unauthorised payment which is made after you told us that your security details are no longer safe.

To be entitled to a refund, you must provide the information reasonably necessary to establish that these Terms have been satisfied. The refund or a reason for refusing it will be provided within 10 business days of the later of your request or receipt of any further information required. If you are not satisfied with the reason for refusing a refund, please contact your local branch or our telephone banking service. If we discover subsequently that you are not entitled to a refund, we will be entitled to reapply the payment(s) to your account, together with any applicable interest and/or charges.

You will not be entitled to a refund where you have given your consent to the payment directly to us and at least 4 weeks in advance:
(a) we or the payee have provided you with information about the payment: or
(b) information about the payment was made available to you via our online banking service, or at any branch.

14. REMOTE BANKING TERMS

a. Introduction

This Term applies if we have agreed that you may use our telephone and online banking services to operate your account.

b. Security procedure

14.2.1 You must keep your security details (which include the identifying words, codes and numbers agreed between us) secret and take all reasonable precautions to prevent unauthorised or fraudulent use of them.

14.2.2 You must not disclose your security details to any other person or record them in any way that may result in them becoming known to another person.
After initial registration we will never contact you. or ask anyone to do so on our behalf, with a request to disclose your security details in full. If you receive any such request from anyone (even if they are using our name and logo and appear to be genuine) then it is likely to be fraudulent and you must not supply your security details to them in any circumstances. You should report any such requests to us immediately.

14.2.3 If you suspect someone knows your security details you must contact us immediately.

14.2.4 You will be responsible for all instructions given by you or anyone acting with your authority between the time you pass the security procedure and the time you exit from our services. Please note that this includes any input errors or instructions sent by anyone but yourself. You should not leave the device you are using unattended while you are logged on to one of our services.

14.2.5 You are responsible for making sure information either stored or shown on your device(s) is kept secure."

key questions

I think the above relevant considerations mean that, if the transactions Mr W disputes were unauthorised, it would be fair and reasonable for NatWest to refund the amount stolen from him, unless, with intent or gross negligence, he failed to comply with the terms and conditions of his account.

I think there are a few key questions that are relevant to my consideration about what is fair and reasonable in the circumstances:

1. Were the disputed transactions authorised by Mr W? and;

2. If they weren't, can NatWest demonstrate that Mr W acted with gross negligence – particularly taking into account the terms and conditions of his relationship with NatWest and the obligations set out in Regulation 57 of the PSR 2009?

were the disputed transactions authorised by Mr W?

Mr W accepts he gave the fraudster the mobile banking app activation code. And I accept this action was a major step in the process which allowed the disputed transactions to be made. But Mr W didn't know, at any time during the call with the fraudster, that any transactions were going to be made from his account. In fact, according to Mr W, he was asked for the code specifically to stop his debit card and online banking and prevent any fraudulent payments going through.

So I don't think it would be correct to say that, by disclosing the code, Mr W consented to or authorised payments being made from his account.

As such, I'm currently minded to say it wouldn't be fair or reasonable to conclude that Mr W authorised the payments. And, actually, NatWest hasn't made this assertion either. So my starting point really is to say that Mr W shouldn't be held liable for them unless I can conclude that he failed with intent or gross negligence to comply with the terms and conditions of his relationship with NatWest, and the obligations set out in the PSR 2009.

can NatWest demonstrate that Mr W acted with gross negligence?

The principal obligation relevant to this case is Mr W's obligation to take all reasonable steps to keep safe the "security details" of his account. His account terms and conditions explain what this means in practice. And, as highlighted above, the section about remote banking warns that the bank will never ask him to disclose his full security details after initial registration and any such request is likely to be fraudulent.

So, I think Mr W was under an obligation not to share information that would enable someone to set up a mobile banking app.

There seems no dispute the mobile banking app was downloaded onto a new device that was in the fraudster's possession. And Mr W gave away the activation code which enabled the fraudster to complete the first stage of the registration process. But that process required more than just the activation code to be disclosed. And NatWest hasn't said Mr W must have shared all the information necessary to do that. The bank has said only that if Mr W hadn't given away the code then the fraudster wouldn't have been able to complete the mobile banking app registration process and get access to his account. To be clear, at no time has NatWest said specifically that it thinks Mr W acted *"with gross negligence."*

With this in mind, I don't agree that just because the fraudster was successful in setting up the mobile banking app, it follows that Mr W acted with gross negligence.

Acting with gross negligence isn't the same as failing to keep security information safe. I think there are ways in which a customer might fail to keep their security information secure which will fall short of being grossly negligent. Gross negligence isn't a term to be used lightly. As I set out earlier, it's more than just being careless or negligent. And the PSR 2009 make it clear that the use of a payment instrument is not *in itself* sufficient to prove that a payer failed with gross negligence to comply with regulation 57.

Gross negligence isn't an abstract concept. It's important to take into account all the circumstances when considering whether an individual's actions amount to gross negligence. I've thought carefully about the actions Mr W took in the circumstances here. I've thought about whether what he did fell so far below the standard of a reasonable person that it would be fair to say he failed with gross negligence to keep his personalised security details safe or to comply with the terms and conditions of his account.

With that in mind, Mr W says he believed completely that he was speaking with a NatWest employee during the call when he disclosed the code. And I can understand, in the circumstances, why the call wouldn't, reasonably, have aroused any obvious suspicions. I say that because:

- Although Mr W had never rung the "0345" number that the call seemed to have come from, his phone used the "SMART" caller ID to assign that number with NatWest's name.
- The "0345" number *was* one of NatWest's own (which is how Mr W was able to use the incoming call record to call the bank back the following morning).
- The caller said he worked for NatWest and asked for Mr W by name. Mr W had more than one account with NatWest, so it wouldn't have seemed unusual for the bank to call him.

So I think, at the time of the call, there was little to make Mr W wary about the person he was speaking with. And I can understand why he'd be worried about the suspicious transaction the fraudster was talking about and why he'd be keen to do what he was told in order to protect his money. I think Mr W's actions must be seen in that light.

NatWest has focussed its decision not to refund the disputed transactions on the fact Mr W gave the fraudster the mobile banking activation code. I acknowledge the text he was sent with the code included the words *"Warning: never reveal this code to anyone".* Mr W said he didn't see this warning because he didn't need to open the full text. That may be so. But even if he had seen it, in the context of Mr W's genuine belief that he was speaking with the bank, and his belief that sharing the code was necessary to safeguard his money, I can't say his failure to pay closer attention to this wording amounted to gross negligence. I don't think he appreciated any risk. Nor do I think he acted with "serious disregard" or "indifference to an obvious risk". Instead, he was acting under the belief that his money was at risk and the person he was speaking with worked for his bank and was helping him protect his account. So I don't think, in the circumstances of Mr W's case, that this could fairly and reasonably be said to amount to gross negligence.

As I've already said, NatWest hasn't put forward any suggestions about how the fraudster was able to complete the mobile banking app registration process, given he needed more than just the activation code to do so. I'm not sure about that either. So I've had to make my decision based on the balance of probabilities, after weighing up the evidence, which includes what Mr W has said about what happened during the call with the fraudster.

It's often useful in this type of case to listen to the very first discussions that took place between the consumer and the bank about the fraud. That call is the closest in time to the fraud, so memories of what happened won't yet have dimmed or been influenced by any conclusions the bank might have subsequently reached. Unfortunately, NatWest no longer has a recording of the second, more detailed part of Mr W's first call to them.

But we do have recordings of subsequent calls and I note Mr W said repeatedly that he gave the fraudster no other personal or banking-related information. When we pressed him about this, he said he couldn't rule out the possibility he might've given away some additional information, but he thinks this would have been limited to the usual security questions a bank asks, like address and date of birth.

Mr W says he's sure he didn't give out any of his online banking security details and he hadn't received or responded to any obvious "phishing" type emails in the days leading up to the call. I think if Mr W had given away any additional information, he'd probably have mentioned this when he first contacted the bank and us. I say that, at least in part, because he admitted from the start that he'd

given away the activation code. But if I'm wrong and if he did give away some additional security details then I think he probably did that, again, because he was under the spell of the fraudster and thought doing so was part of the usual security process.

I've also thought about the warnings that're included in the remote banking section of the terms and conditions (specifically 14.2.2), the reference at 4.5.5 to a consumer's liability if they've failed to keep their security details safe and the other information NatWest says it's shared generally with customers about spotting scams. With the latter in mind, I acknowledge what it's done is good practice, with consumer protection in mind. And increasing levels of consumer awareness may, in some cases, help to prevent frauds like this from succeeding. But I also have to take into account that such warnings are not always read by consumers. And, even if they are, they may not be at the forefront of a consumer's mind when faced with a sophisticated real-time confidence trick of this nature. So I don't think it would be fair or reasonable to say Mr W was grossly negligent by failing to connect any messages or warnings he might have seen to a situation when he was under stress and when he was reasonably under the impression that he was talking to his own bank.

Mr W was persuaded to divulge a security code to a fraudster as part of a sophisticated and successful scam. But I don't currently think NatWest has shown he acted with gross negligence. On the evidence I've seen so far, I don't think Mr W's actions amounted to gross negligence.

Should NatWest have done things differently after Mr W reported the fraud?

I've considered carefully the way the bank handled Mr W's initial concerns and related complaint – this has included listening to some of the phone calls he made to the bank.

If fraud like this is reported quickly enough and the bank acts promptly, it's sometimes possible to ring-fence and/or retrieve some the money that's been taken. And that would be of benefit to both the bank and its customer. With that in mind, NatWest says it tries to make this sort of contact within 24 hours of the fraud being reported, but there's no guarantee of success.

As noted above, some of Mr W's money was transferred to another bank. And NatWest's records show it got in touch with that bank within two hours of finding out about the fraud. But, unfortunately, the receiving bank said the money had already been withdrawn or moved elsewhere. It's not clear when exactly Mr W's money was taken from the receiving account and so it's possible, if the bank had called sooner, that some of it might have been retrieved and returned to Mr W. But I think the bank acted within a reasonable amount of time calling, as it did, within two hours of being told about the fraud.

Two other transfers, totalling £150 were made to another account with NatWest and I've seen nothing to suggest the bank similarly checked that account with a view to retrieving Mr W's money. I've seen a statement for the receiving account which shows a total of £130 being withdrawn and transferred the same day the money arrived in the account. And, again, it's not clear when exactly that happened. But there was a little over £37 remaining in the account at the end of 30 October. Yet the bank did nothing, as far as I can see, to ring-fence that or return it to Mr W. That would've been a small proportion of the amount that was taken from Mr W, but it would have been something and would have limited the amount that NatWest will likely have to pay Mr W as a result of my decision.

Mr W also says he's unhappy NatWest said it would report the matter to the police but didn't do so. But I can't see it promised to do that. And, in any event, the bank's records suggest Mr W did this himself and called the bank the day after he first reported the fraud to let it know.

Mr W says the bank's staff were rude and insensitive – they apparently said the fraud was his fault and told him to stop calling. NatWest has given me a number of call recordings and I can see it explained why it wouldn't refund the money and explained how long it would take to consider Mr W's appeal. Mr W kept calling the bank because he didn't agree with its decision but I can understand why the bank may have told him this wasn't necessary – it needed time to look further into his concerns and would have had other, similar complaints to deal with. I think it's likely the reason it told Mr W he

needn't keep calling was because he didn't have any new information to share and the bank didn't want him wasting his time.

NatWest told Mr W during one call that it could take up to 56 working days to look into his complaint. But it didn't end up taking anywhere near that long. The complaint was raised on 30 October 2017 and the bank sent Mr W its final response on 15 November 2017.

The bank has paid £50 compensation to Mr W already and, overall, I think that's a fair amount to reflect the upset caused by its complaint handling given the circumstances.

fair compensation

For the reasons given, I don't think it was fair or reasonable for NatWest to refuse to refund to Mr W the amount stolen from him. And I currently think, to fairly compensate him, NatWest should:

3. Credit Mr W's current account with £780. In making this refund the bank, in accordance with the terms and conditions applicable to Mr W's account, is entitled to withhold up to £50. If it exercises this right, I consider it would be fair and reasonable for it to inform Mr W of its decision to do so.

4. Add interest from the date of the disputed transactions to the date of settlement at the rate Mr W would have received had the money not been moved from his ISA account into his current account and removed by the fraudster. That interest would have been paid gross because the money was in an ISA. But if NatWest thinks it must deduct tax from the interest element of this award, it should provide Mr W with the appropriate tax deduction certificate.

provisional decision

Cases such as Mr W's are a good example of the kind of finely balanced decisions I have to make in circumstances where I can't know for sure everything that has occurred – decisions that I must make on the balance of evidence, fairly and reasonably. But, for all the reasons I've set out above, I think it's fair and reasonable to tell National Westminster Bank Plc to reimburse Mr W's loss.

My provisional decision is that I'm minded to uphold this complaint. My current view is that National Westminster Bank Plc should calculate and pay compensation as set out above.

Ruth Hersey
ombudsman