DRN-2605137

The complaint

Miss Z is unhappy with Nationwide Building Society's response to her complaint after she fell victim to a scam. It declined to reimburse the money she lost after being tricked into sending £53,500 to an account controlled by a fraudster.

What happened

I issued my provisional decision on this complaint on 1 February 2021. The background and circumstances of the case and the reasons why I was minded to uphold it were set out in that decision. I have reproduced the provisional decision in italics below:

In October 2019 Miss Z was in the process of purchasing an apartment which she intended to rent out. She was in regular contact with her solicitor, and the sale became particularly time pressured as Miss Z and her partner were beyond the initial agreed deadline for paying the £53,500 deposit on the property, due to a delay in receiving funds via a remortgage. This meant that Miss Z's solicitor was regularly sending her emails asking her to make the necessary payment as quickly as possible so as not to risk losing the property.

At the end of October, the 8 November was proposed as an agreed date for exchange. On 4 November Miss Z emailed her solicitor to reassure her things were continuing to progress and that she hoped to have received the remortgage funds by 8 November, which would enable them to pay the deposit and exchange. But Miss Z asked whether, if the release of the remortgage funds was delayed, she could pay £20,000 (which was pretty much all her and her partner's savings) and then the remaining amount a few days afterwards.

Miss Z's solicitor replied, explaining that the seller's solicitor had confirmed the seller expected a payment of £20,000 on exchange, with a further payment of £33,500 on or before 12 November. She told Miss Z that if she agreed, the following would need to be added to the contract

"Deposit £20,000 on exchange with £33,500 to follow on or before 12 November. If the Buyer fails to make payment of the £33,500 by 12 November the Seller reserves the right to deem the Agreement breached by the Buyer with all monies paid to that date (including all deposits) being retained by the Seller".

Miss Z's solicitor asked her to confirm whether she was happy to proceed with the exchange on this basis, if she was unable to pay £53,500 by 8 November.

On 7 November Miss Z sent evidence to her solicitor from a different bank to show that the remortgage was almost complete. Unfortunately, the response Miss Z received to this email was from a fraudster, who had somehow managed to start impersonating Miss Z's solicitor.

The fraudster told Miss Z that the evidence was 'fair enough' but that Miss Z should go ahead and pay £20,000 'today' to avoid any potential delays (presumably in making the payment) on 8 November. Miss Z was not surprised to receive this email given the amount of contact she'd received from her genuine solicitor about paying the deposit as soon as possible, and so she responded asking for the relevant bank account details. The fraudster

gave her account details which didn't belong to the solicitor.

Miss Z initially made two payments of £10,000 to the fraudster on 7 November 2019. Miss Z has explained the payment of £20,000 was paid in two instalments because the maximum she believed she could transfer in one go via online banking was £10,000.

Miss Z received the funds from the remortgage (£55,122.95) on 8 November 2019. She then proceeded to pay the rest of the deposit in 4 payments on 11 November 2019 (three payments of £10,000 and one payment of £3,500) reflecting her understanding of the payment limits.

It wasn't until 18 November 2019 that Miss Z realised she'd fallen victim to a scam. At that point Miss Z noticed that the email from the fraudster contained one different digit to the genuine solicitor's email – an 'i' rather than an 'l'.

Miss Z notified Nationwide that day. Nationwide contacted the recipient bank to try and recover the funds but unfortunately no funds remained. Miss Z complained to Nationwide. She was aware of the Contingent Reimbursement Model Code (CRM code) and believed she was entitled to be refunded for the money that she'd lost.

Nationwide didn't uphold her complaint. It didn't think it should reimburse Miss Z under the CRM Code. In its final response Nationwide explained that at the time Miss Z made the payments to the fraudster she was shown tailored warnings which were designed to prevent a scam. It also explained to Miss Z that faster payments offered no protection – that they are like cash payments - and suggested making future purchases with a debit or credit card, given they do offer a level of protection.

Miss Z remained unhappy with Nationwide's position and so she referred her complaint to our service. She explained that at the time she made the payments she felt under pressure as the seller was ready to pull out given the delay in paying the deposit. She acknowledged Nationwide had sent her a copy of the 'Little Book of Scams' after the scam, but she explained this would've been more useful prior to the scam occurring.

Miss Z also told us she'd been badly affected by the scam – suffering with anxiety and insomnia, and that she'd been prescribed medication to control her symptoms. As a result of the scam she'd lost the property purchase, her partner and she had lost their life savings, lost the reservation fee of £2,500 and she says she couldn't afford Christmas presents for their daughter.

We asked Nationwide for its submissions.

It explained that as it had warnings in place to try to protect her from this type of scam it wasn't liable for her loss. It had considered whether it ought to reimburse Miss Z under the provisions of the CRM Code and didn't think it did. That was on the basis it believed Miss Z had ignored effective warnings and so hadn't met her requisite level of care.

An investigator looked into Miss Z's complaint and upheld it. She didn't think the warning would've been impactful in the specific circumstances of the case and so Nationwide shouldn't have decided not to reimburse Miss Z. She also felt that given the nature of the payments, Nationwide ought to have contacted Miss Z to check she wasn't at risk of financial harm - and had it done so, she believed the scam could've been prevented.

In response to the view, Nationwide asked us for further information about the scam. It explained it wanted to get a better picture of:

- *the communication between the genuine solicitor and the fraudster; and*

- *why Miss Z believed she was led to believe she was paying the same organisation.*

And so it asked to see copies of the emails between Miss Z and her genuine solicitor, and Miss Z and the fraudster.

The investigator shared this evidence with Nationwide. Nationwide subsequently disagreed with the view. In summary it said it has provided a clear warning to the customer about the specific scam risk which subsequently materialised, and recommended an action which, if taken, would've prevented the scam. As a result, it clearly satisfied the requirements of an Effective Warning set out in the CRM Code and Miss Z simply ignored the warning. Therefore it wasn't fair that it should be held responsible for her loss.

It made the following key points in support of its view which I've separated into Nationwide's thoughts on the intent of the CRM Code, Effective Warnings, whether Miss Z had a reasonable basis belief she was making a legitimate payment, and out of character and unusual transactions.

<u>Nationwide's key points in response to the view</u>

The intent of the CRM Code

- *The CRM Code has the following overarching objectives:*
  (1) to reduce the occurrence of APP scams;
  (2) to increase the proportion of Customers protected from the impact of APP scams, both through reimbursement and the reduction of APP scams;
  (3) to minimise disruption to legitimate Payment Journeys
  At the outset the CRM Code therefore recognises a balance between the desire to reduce the incidence of APP scams and minimising disruption to the millions of legitimate payments made by the signatory Payment Service Providers (PSPs) each day. This is important as it implicitly recognises that the objective of the Code is not to prevent every scam occurring or to unduly disrupt legitimate payment journeys.

- *Reimbursement of customers is only one way in which the CRM Code seeks to protect customers from the impact of APP scams. Since the introduction of the CRM Code (and in recent years generally), Nationwide (and other PSPs) have made significant improvements to their fraud detection and warnings systems, resulting in substantial numbers of potential scams being stopped before monies were lost.*

- *It notes that the view says "Under the CRM Code the starting principle is that a firm should reimburse a customer who is victim of an APP scam (like Miss Z) except in limited circumstances" but that is not what the Code states or intends. Whilst it accepts that R1 is drafted from the perspective of the PSP being liable unless an exception is applied, it cannot be intended to alter the balance of the three overarching objectives, which reflects the reality that for payments systems to properly enable customers, payment journeys should not be made overly complex and nor should large numbers of payments be stopped as a matter of course.*

Effective warnings

- *Whilst a degree of specificity in the warnings is required, Effective Warnings are not expected to be tailored to the precise circumstances of the customer and the payment. The warnings should be "risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified" and "tailored to the customer type and the APP scam risk identified", not the scam itself.*

- *The warning was effective, in accordance with SF1(2) of the Code, for the following reasons:*

- *The warning was given during the payment journey, before the payments were authorised*
- *It was specific, risk-based and tailored to the APP scam type which customers who believe they are paying a bill, invoice or monies for a property sale face - it accurately reflected the situation Miss Z was in. Despite this, whether or not the warning was applicable to her precise circumstances is not a sustainable basis on which the warning can be judged to be effective or not.*
- *The warning enables a customer to understand what action they should take to avoid the risk of fraud;*
- *The warnings are understandable and clear; and*
- *The warnings are impactful - they are concise but contain clear information about the risks the customer faces and what they should do to avoid those risks, in short sentences, which the customer should easily understand.*

- *The warning Miss Z received was direct and specific:*

- *The bold heading to the warning asked "Have you double-checked these bank details with the payee directly?" Miss Z would immediately have been aware that she had not double checked the details – and that she should do so. She chose not to do so.*
- *The first sentence in the body of the warning is again specific to her circumstances:*
  "Scammers pose as genuine organisations and trick people to transfer money to fraudulent accounts." That is exactly what happened in this case and should have reinforced the point in bold above.
- *The warning continues: "If these bank details are new, or have recently changed, give the payee a call to double-check them. Always use the number on their official website." Here the account details were new to Miss Z, so again this should have reinforced the key message.*
- *There was a very clear warning regarding the consequences of proceeding without heeding this advice: "Remember, you'll lose your money if you agree to transfer money upfront for a deposit, item, or service and it doesn't work out."*

Reasonable basis for belief

- *What is reasonable in the circumstances depends in part on the context in which the events took place. A key part of that context is the information given to Miss Z by her solicitor. The solicitor's email of 5 November 2019 (before the payments were made) contained the following warning: "Please note we have been made aware that fraudsters have attempted to persuade a client to send funds to another account. We will never change our bank details and will not provide those details in an open email. Please check with us directly by phone or use the Safebuyer Scheme before sending us any monies as we will not be responsible for any lost funds."*

- *Miss Z should therefore have been aware of the possibility of precisely the scam which occurred, and been highly vigilant during the payment process.*

- *This specific warning also supported the effective warning given in the payment process, as set out above, as it was entirely consistent with it.*

- *The change in email address is subtle, but given the repeated warnings which had been provided to Miss Z, she should have been extra vigilant and examined the*

email in depth.

- *The change in the email address is also important because it confirms that the real solicitor's email account wasn't compromised. Nationwide has confirmed that Miss Z's email address was included in a 2018 data compromise of email addresses, user names and passwords for a fitness app. Therefore, it appears likely to Nationwide that Miss Z used the same password for her email account and the app so the compromise of the fitness app led to an unauthorised access to her personal email.*

- *At the time of the breach, the fitness app sent out this advice to all affected customers, advising them to change their passwords linked to their accounts. It's more likely than not Miss Z didn't take the suggested action and if she had the scam would most likely not have happened. And even if she had changed her password promptly, Miss Z would've been aware her email account had been compromised and should've been on heightened alert, especially when considering the warnings she received from Nationwide and her solicitor.*

Out of character and unusual transactions

- *We have failed to take into account that the payments were for a deposit for a house. It is not at all unusual for our customers to make occasional (entirely legitimate) payments connected with property transactions in this way. Miss Z correctly informed Nationwide that the payment was for a 'bill, invoice or property sale', which is entirely consistent with her behaviour.*

- *Our view that it would be reasonable to disrupt these payments would mean that Nationwide should intervene in all situations where a property deposit is being paid in this way. That would be a significant burden (and cost) for Nationwide, and the disruption could potentially cause detriment for customers. There is nothing in the CRM Code that suggests a written warning is insufficient and there is no mention in the CRM Code of a requirement for outbound calling.*

- *Finally, it notes the information which we believe would have been conveyed to Miss Z by telephone, had it intervened before processing the payment, is precisely that which Nationwide provided in the warning, and which Miss Z ignored. It doesn't agree that conveying the information by a different method would have resulted in Miss Z telephoning her solicitors to check.*

We shared the substance of Nationwide's submissions with Miss Z who has told us the following:

- *Miss Z did see the warnings and did read them carefully, but as she was already corresponding with the solicitors on a regular basis she didn't think the warning applied to her situation; at no point did she receive a random, unexpected email asking her to transfer money to new details.*

- *Her genuine solicitor had been regularly emailing her to find out when she'd be paying the deposit and she felt under pressure to make the payment as soon as she could to prevent the sale falling through – they were already outside of the 30 day payment period – so it came as no surprise to receive another email asking for a payment to be made.*

- *Miss Z explained that she'd thought about it all for so long and whether she could've done things differently. But she satisfied herself that the email had arrived in a*

genuine email chain, there were no red flags, the tone of voice was the same, the signature was the same etc. Miss Z has said that she was the one driving everything in her head – she was not sent a random email containing bank details, asking for money. It was Miss Z that had asked for those details and it was her that was in control.

- *The emails from the fraudster were sent to Miss Z, her partner and the sales manager and none of them realised the email wasn't genuine*

- *Miss Z did read the disclaimer at the foot of the genuine solicitor's emails the first time she saw it. She didn't read the disclaimer everyday – instead her eye was drawn to the facts within the body of the email*

- *It was make or break whether the sale of the property would be completed – Miss Z felt under pressure due to the time constraint*

- *Miss Z has evidence that her email account wasn't compromised.*

Miss Z accepted the investigator's view but Nationwide has asked for an ombudsman to consider the complaint. The case has therefore been passed to me.

What I've provisionally decided – and why

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

In deciding what's fair and reasonable in all the circumstances of a complaint, 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 be good industry practice at the time.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

However, where the consumer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.

Of particular relevance to the question of what is fair and reasonable in this case is the Lending Standards Board's Contingent Reimbursement Model for Authorised Push Payment Scams (the CRM Code) – a voluntary code of practice which Nationwide has signed up to and committed to follow. And I have thought carefully about how the CRM Code applies to the payments Miss Z made.

The CRM Code

The CRM Code is a voluntary code issued by the Lending Standards Board in May 2019 following development and consultation by the APP Scams Steering Group - a group established in February 2018 by the Payment Systems Regulator and made up of representatives from the payment industry and consumer organisations, as well as observers from regulators, government and law enforcement.

The September 2018 APP Steering Group Draft Reimbursement Model Code Consultation

Paper explained the background to, and aims of, the CRM Code:

"1.2. In September 2016, the consumer body Which? submitted a super-complaint to the Payment Systems Regulator (PSR) about APP scams, raising its concerns that victims do not have enough protection. The PSR investigated the issue and the concerns raised, and in December 2016 found that more needed to be done to tackle APP scams. The PSR and industry undertook further work, and in November 2017, the PSR published the findings and outcome of this work. This included a consultation on the introduction of a Contingent Reimbursement Model (CRM). The model sets out the circumstances in which payment service providers (firms) would be responsible for reimbursing APP scam victims who have acted appropriately. In February 2018, after taking the consultation responses into account, the PSR considered a CRM – formalised into a voluntary industry code of good practice – is an effective way to reduce the occurrence of APP scams and the devastating harm they cause consumers.
…
1.5 The main aim of the Code is to reduce the occurrence of APP scams from happening in the first place, and lessen the impact these crimes have on consumers, microenterprises and small charities (referred to as customers – see paragraph 3.24). The steering group considers that the draft code should achieve this. It incorporates existing good industry practice for preventing APP scams and helping these customers protect themselves from these crimes, while ensuring customers remain vigilant….
…
3.10 The code should incentivise the parties involved to take action to prevent and respond to APP scams where they are best placed to do so. Firms should be incentivised to implement and use measures that effectively prevent and assist with the response to APP scams, and customers should be incentivised to remain vigilant. This should help minimise the number of APP scams as more is done to stop them happening in the first place. When APP scams do happen, reimbursing the victims – where they could not have reasonably protected themselves – reduces the customer harm."

Those aims are reflected in the CRM Code's overarching provisions and in the structure of the CRM Code itself, which sets our both the standards that firms like Nationwide should meet and the circumstances in which a customer that has been a victim of an APP scam should be reimbursed.

<u>When should a customer be reimbursed under the CRM Code?</u>

The starting proposition under the CRM Code is that a customer will be reimbursed if they are the victim of an APP scam. But – except in cases where a customer is vulnerable to APP scams – a firm may choose not to reimburse (at its discretion) if it can establish that one of the five specified exceptions to reimbursement apply.

This reflects the reimbursement principle, set out at various points within the APP Steering Group's consultation paper and policy statement, that the victims of APP scams who have met the requisite level of care should be reimbursed.

For example, the September 2018 draft CRM Code consultation paper explained:
3.46. The code reflects the proposed reimbursement principle that victims of APP scams who have met their requisite level of care should be reimbursed…
3.47. The code sets out a requisite level of care for customers to help protect themselves from APP scams….
3.48. The steering group has been able to identify a number of matters that appear

essential to good decision-making by customers. They are set out in R2(1)(a) to (g), explained below. These matters may turn on how firms behave towards their customers, including the tools they give to their customers.
3.49. The steering group has designed the provisions governing reimbursement of victims so that it is presumed that a victim will be reimbursed unless good reasons can be established that the customer should not be – in other words, the customer did not meet its requisite level of care…
3.50. The provisions at R2 set out the circumstances in which a firm may choose not to give a reimbursement, which may depend on the firm's compliance with the standards under the SF provisions.
3.51. Just as firms will need to consider whether or not a particular standard under the SF provisions would have had a material effect on preventing the APP scam that took place (see above at paragraph 3.28), in establishing whether a customer should be reimbursed, firms need to consider whether what the customer did would have had a material effect in avoiding the APP scam.
3.52. In assessing whether a customer has met the requisite level of care and should be reimbursed, firms may take a number of matters into account. These are specifically related to steps customers should take to help protect themselves from APP scams.
3.53.R2(1)(a) and (b) - firms will have to establish compliance with the effective warnings and Confirmation of Payee standards before they can establish that a customer ignored the tools given to help them protect themselves.

And in the 28 February 2019 Feedback on Responses to Consultation Paper, the APP Steering Group said:

1.7 The Steering Group has concluded that where customers of PSPs who have signed up to the Code meet their requisite level of care, they will be reimbursed. This includes in the scenario where both the consumer and PSPs involved in the transaction have met their expected level of care (the 'no blame' scenario).

Under the CRM Code itself, the firm's actions may be relevant to the question of whether the consumer has met the requisite level of care required for reimbursement. But it is important to note that does not automatically follow from the fact that a firm has met the standards for firms that the consumer may not be reimbursed. The question which determines whether a firm may choose not to reimburse is whether the consumer has met the requisite level of care?

<u>The exceptions to reimbursement</u>

The CRM Code says that (so far as the potential exceptions to reimbursement are relevant to this complaint):

"Principle
R1 Subject to R2, when a Customer has been the victim of an APP scam Firms should reimburse the Customer

Exceptions
R2(1) A Firm may choose not to reimburse a Customer if it can establish any of the following matters in (a) to (e). The assessment of whether these matters can be established should involve consideration of whether they would have had a material effect on preventing the APP scam that took place.
(a) The Customer ignored Effective Warnings, given by a Firm in compliance with SF1(2), by failing to take appropriate action in response to such an Effective Warning given in any of the following:
(i) when setting up a new payee;

(ii) when amending an existing payee, and/ or
(iii) immediately before making the payment
(b) …
(c) In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that: (i) the payee was the person the Customer was expecting to pay; (ii) the payment was for genuine goods or services; and/or (iii) the person or business with whom they transacted was legitimate.
(d)…
(e) The customer has been grossly negligent. For the avoidance of doubt the provisions of R2(1)(a)-(d) should not be taken to define gross negligence in this context."

I have not set out the other matters in full. But it is important to note that a firm may choose not to reimburse if it can show any one of the listed exceptions to reimbursement apply (unless the consumer was vulnerable to APP scams).

The application of the CRM Code to Miss Z's case – effective warnings

Nationwide says that it is entitled not to reimburse Miss Z under the provisions of the CRM Code because she failed to take appropriate action in response the warnings it gave her when she made six payments totalling £53,500 out of her account.

Given the provisions of the CRM Code, I must therefore consider:

1. Whether the warning(s) Nationwide gave Miss Z were 'effective warnings' given in compliance with SF1(2)?

2. If so, whether Mrs Z 'ignored' those effective warnings by failing to take appropriate action in response to the warnings?

3. And if so, whether taking appropriate action would have had a material impact on preventing the APP Scam which took place?

I will consider each question below. If the firm cannot establish that each requirement has been met, then the exception to reimbursement does not apply under the provisions of the CRM Code.

1. Whether the warning Nationwide gave Miss Z was an 'effective warning' given in compliance with SF1(2)?

SF1(2) says:

Where Firms identify APP scam risks in a Payment Journey, they should take reasonable steps to provide their Customers with Effective Warnings, which should include appropriate actions for those Customers to take to protect themselves from APP scams.
(a) Firms should take reasonable steps to make their Customers aware of general actions that could be taken to reduce the risk of falling victim to an APP scam
(b) Where the Firm identifies an APP scam risk, it should provide Effective Warnings to customers. This may occur in one or more of the following:
(i) when setting up a new payee
(ii) when amending an existing payee; and/or
(iii) during the Payment Journey, including immediately before the Customer authorises the payment, before the Customer's account is debited

(c) Effective Warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the Customer is initiating the payment instructions
(d) Effective Warnings should enable the Customer to understand what actions they need to take to address the risk, such as more appropriate payment methods which may have additional protections, and the consequences of not doing so.
(e) As a minimum, Effective Warnings should meet the following criteria
(i) Understandable – in plain language, intelligible and meaningful to the Customer
(ii) Clear - in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's Principles for Businesses
(iii) Impactful – to positively affect Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. This should include steps to ensure that the Customer can reasonably understand the consequences of continuing with an irrevocable payment;
(iv) Timely – given at points in the Payment Journey most likely to have impact on the Customer's decision-making;
(v) Specific – tailored to the customer type and the APP scam risk identified by analytics during the Payment Journey, and/or during contact with the Customer.

I am mindful that in the September 2018 consultation the APP Steering Group said:

"Prevention
3.32 These provisions are about helping customers to help protect themselves from falling victim to APP scams. There are two main strands – Confirmation of Payee, which is discussed further below and providing effective warnings to customers during payment journeys.
3.33 The steering group wants to incentivise those with the expertise and ability to prevent APP scams effectively, and to reduce its impact. Therefore, the code sets a standard for firms to use their expertise to provide their customers with effective information, at key stages in a payment journey, so that customers have a better chance to protect themselves against being defrauded.
3.34. To do this, at SF(2) there is a proposed framework for firms to provide effective warnings to their customers. As part of this, there are five minimum criteria (at SF1(2)(e)) that effective warnings should meet. They should be:

- *Understandable – in plain language, intelligible and meaningful to the Customer;*
- *Clear - in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's Principles for Businesses;*
- *Impactful – to positively affect Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. This should include steps to ensure that the Customer can reasonably understand the consequences of continuing with an irrevocable payment;*
- *Timely – given at points in the Payment Journey most likely to have impact on the Customer's decision-making;*
- *Specific – tailored to the customer type and the APP scam risk identified by analytics during the Payment Journey, and/or during contact with the Customer.*

3.35. A constituent element of an effective warning should be that the customer is given clear guidance about action they should take to help avoid the risk that they might be about to fall victim to an APP scam. The customer should also be made fully aware of the consequences if they do not follow those actions and proceed with the payment. That is, that they might not be reimbursed. The warning should also notify the customer whether other payment methods which may be more appropriate to their circumstances are available – for example where a customer is using an online

market platform that they might want to pay through that platform."

I am satisfied that under the CRM Code, whether or not a warning is effective in compliance with SF1(2) will depend on a number of factors:

- *The warning must as a minimum meet the UCITS criteria (understandable, clear, impactful timely and specific). As these are minimum criteria, it may be necessary for the warning to do more than just meet the UCITS requirements to amount to an effective warning – it would not be an effective warning if the information provided did not give the customer a better chance to protect themselves against being defrauded.*
- *The warning should include appropriate actions for customers to take to protect themselves from APP scams and they should enable customers to understand what actions they need to take to address the risk of APP fraud, such as more appropriate payment methods which may have additional protections and the consequences of not doing so.*

Nationwide has said it met its standards and provided effective warnings that met the definition set out in SF1(2)(e). In particular, it has said the first warning accurately reflected the situation Miss Z was in.

It's accepted that Miss Z selected the 'Bill, invoice or property sale' option as a reason for the payments she made, after which she was presented with:

"STOP AND THINK
Have you double checked these bank details with the payee directly?
Scammers pose as genuine organisations and trick people to transfer money to fraudulent accounts. If these bank details are new or have recently changed, give the payee a call to double check them. Always use the number of their official website.
Common scams include cold calls and emails requesting you transfer money. If you've been contacted in this way, this is likely to be a scam and you should stop this now.
Remember, you'll lose your money if you agree to transfer money upfront for a deposit, item or service and it doesn't work out. Pay with a debit or credit card when you can instead."

Given the payment reason option that sat behind the warning, I'm satisfied Nationwide intended on providing Miss Z with warnings that aimed to prevent her falling victim to email and invoice intercept scams (amongst other scams). Email or invoice intercept scams are where a fraudster hacks into email communications between two people – often a client and a company – and email the client, disguised as the company, (or in this case a solicitor), informing them that the bank details have changed, or they proactively provide account details belonging to a fraudster. A key feature of this type of fraud is that the fraudster targets customers who are already expecting to pay a bill, solicitor etc.

It seems to me this was the scam risk Nationwide had identified and of course this was the type of scam Miss Z fell victim to. I've therefore thought about whether the warning was effective, bearing in mind the scam risk that Nationwide had identified.

Having considered the warning very carefully, I'm not persuaded it was sufficiently impactful or specific to amount to an 'effective warning'. I'm not persuaded it's more likely than not that the warning Nationwide provided in this case would positively affect customer decision making in the way required by the CRM Code. In reaching that conclusion I am mindful that:

- *The warning, in my view, does nothing to bring to life the most common feature of this type of scam – that is, that the fraudster is able to convincingly impersonate a recognised contact by email (such as a client, solicitor or tradesman), by intercepting*

a chain of emails, or sending an email from an email address which is the same as, or almost identical to, the genuine email address. While the warning does explain scammers 'pose' as genuine organisations, I'm not satisfied the average customer would understand that 'posing' could be as sophisticated as I've described.

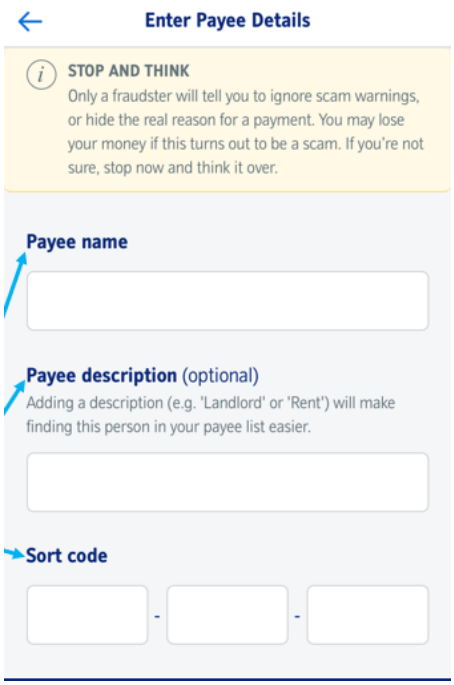
- *The warning describes common scams as including 'cold calls and emails requesting the transfer of money'. It says that 'If you've been contacted in this way this is likely to be a scam...'. This suggests contact is usually unexpected, whereas the reason invoice/email intercept scams are so successful is often because the customer is expecting to make the payment. The description of these 'common scams' would offer some reassurance to customers who have not received a cold call or unexpected email requesting the transfer of money. While it's not clear the intent was to suggest the 'email' referred to in the warning would be 'unexpected', the fact that it follows 'cold call' would suggest, in my view, to the average reader that this would be the case.*

- *Nationwide has specifically recognised the risk of conveyancing scams given it encourages those making a property purchase to have sight of this warning. I therefore think it's unhelpful to use language such as 'genuine organisations' – instead the warning could better bring to life the type of individuals who are most commonly impersonated. It's also possible that consumers wouldn't consider their solicitor to be an organisation.*

- *I think the heading in the warning in bold '**Have you double checked these bank details with the payee directly?'** is meant to grab the consumer's attention, but there is a real risk a consumer might lose interest in reading the rest of the warning because at that moment they're convinced they're already talking to the payee directly.*

In my view effective warnings would need to be impactful enough to overcome, or at least attempt to overcome, the typical features of the type of scam it was seeking to prevent. For the reasons I've explained, I'm not persuaded this particular warning was impactful or specific enough (in line with SF1(2) iii and v) to overcome the typical features of an invoice/email intercept scam.

Nationwide provided a second warning which Miss Z would've seen after selecting 'I'm happy to continue' on the first warning, which said:



I don't consider the second warning to meet the minimum criteria of an effective warning because I don't think it was presented clearly (in line with SF1(2)e ii) or with enough prominence to be impactful (in line with SF1(2)e iii). This is because the warning text was pale grey and set out against a pale yellow background, and the boxes the customer had to fill in in order to complete the payment process were much more prominent, encouraging the eye to look at these boxes rather than anything else. It also wasn't particularly relevant to the type of scam. Overall, I think the second warning is easy to overlook and as a result I don't think that it was clear, specific or impactful and so it doesn't meet the definition of an Effective Warning.

I accept Nationwide feels strongly that it provided effective warnings which met the criteria in SF1(2) e, but overall I don't think the warnings Nationwide provided were sufficiently specific or impactful to break the spell of the type of scam Miss Z fell victim to. So I'm not persuaded it provided effective warnings in compliance with SF1(2), which means the 'effective warning' exception does not apply. But for completeness I have gone on to consider the other parts of the effective warning exception test.

2. Whether Miss Z ignored that effective warning by failing to take appropriate action in response to the warning?

The question posed by the reimbursement section of the CRM Code is whether the customer ignored an effective warning by failing to take 'appropriate action' in response. The way the 'effective warning' criteria is drafted means that a warning does not necessarily need to respond to every feature or nuance of a scam in order to comply with SF1(2). This reflects the fact that the 'effective warning' requirements are found in the standards for firms and are prevention measures that firms are expected to take to reduce the occurrence of APP scams by giving customers information to help them protect themselves from APP scams.

And whilst the list of minimum requirements includes criteria that requires some connection between the warning and the particular scam type to be effective, it is possible that a particular feature of a scam will render a warning meeting the SF1(2) criteria ineffective in reality for the individual customer in all the circumstances. This means a customer might reasonably continue with the payment, notwithstanding the warning they have been given.

Given the background and context to this reimbursement exception and the over-arching principle that lies behind the CRM Code – that the customer should be reimbursed except where they fail to meet the requisite level of care, I'm satisfied that in considering whether the customer 'ignored an effective warning by failing to take appropriate action in response to the warning, it is necessary – if applying the CRM Code correctly – to take into account the particular circumstances of the scam in which the warning was given and of the customer, and what action (or lack of) it would have been reasonable for a customer to take in those circumstances. In other words, appropriate action means considering whether the customer failed to act reasonably in response to the warning.

If this were not the approach required by the 'effective warning' exception, it could lead to the perverse and unintended outcome, that:

- *A customer who is provided with an effective warning meeting the requirements set out in SF1(2), but one that was ineffective in the particular circumstances of a scam, would not be reimbursed despite the customer acting objectively reasonably throughout.*
- *A customer who received a warning meeting the criteria at SF1(2) could continue to have a legitimate basis for believing the transaction to be genuine in all the circumstances (including taking into account the warnings they were given) and so would meet the requisite level of care required by the 'reasonable basis for belief' exception at R2(1)(c). But, it would be open to the firm to deny reimbursement based on the same warning under the 'effective warning' exception at R2(1)(a) notwithstanding that the consumer had a reasonable basis for not acting on the warning in the way intended by the firm.*

I am also mindful that the Practitioner Guide to the CRM Code which was drafted by the LSB 'to support Firms in achieving the requirements of' the CRM Code would seem to support that construction of the CRM Code (although I am mindful that the Practitioner Guide is not intended to be prescriptive nor binding on firms).

The Practitioner Guide explains that in deciding not to reimburse a customer because they ignored an effective warning, firms 'should have regard to the characteristics of the Customer and the complexity and sophistication of the APP scam in determining whether it would have been reasonable for the Customer to undertake the actions identified in the warning'. The practitioner guide goes on to say that 'where there is evidence to suggest that a warning may have been ignored Firms should fully investigate the reasons why.' It further explains that in doing so, firms should have regard to the customer's situation, and the controls they have in place to encourage the customer to heed the contents of the warning – such as using friction points such as delayed payments to give customers the time to consider and digest a warning. And that they should be alert to any indications that the customer may have been in a/is in a vulnerable situation.

The relevant passage says:

"In refusing a claim for reimbursement, Firms should be able to satisfy themselves that the Customer had disregarded the Warning that had been provided to them or failed to take appropriate actions to validate the authenticity of the payment, where the warning instructed them to do so. This may include validating account details being used for payments, or where the scammer purports to be from a recognised organisation, the attempts made by the Customer to validate the identity of the payment recipient. Firms should have regard to the characteristics of the Customer and the complexity and sophistication of the APP scam in determining whether it would have been reasonable for the Customer to undertake the action/s identified in the warning for example, whether the Customer was vulnerable.

Where there is evidence to suggest that a warning may have been ignored Firms should fully investigate the reasons why. In assessing the reasons why a Customer may have ignored a Warning, Firms should have regard to the Customer's situation, and the controls they have in place to encourage the Customer to heed the contents of the warning. This may include for example, the use of friction points such as delayed payments to provide Customers with the time to consider and digest the Warning presented to them. Firms should be alert to any indications that the Customer may have been in a/is in a vulnerable situation and could benefit from additional support. This could stem from an inability to comprehend the contents of the Warning due to limited financial or mental capacity, reducing their ability to make or communicate an informed decision.

Firms should consider this in the context of the Customer's circumstances, including the complexity and sophistication of the scam and the Customer's relationship with the payment recipient, when carrying out their assessment of whether a Customer is vulnerable under R2(3)."

I have considered whether Miss Z failed to take appropriate action in response to the warning(s) she received given the particular circumstances of the APP fraud she fell victim to.

When Miss Z was presented with the warnings, from Miss Z's perspective:

- *She'd been regularly communicating with her solicitor about the need to pay the deposit as soon as possible. Therefore, when she received a further email from who she believed to be her solicitor, asking for a payment to be made, around the agreed date, Miss Z wasn't in any way surprised – the contact was expected.*
- *The email from the fraudster appeared within a chain of emails to the genuine solicitor with only a very minor difference to the email address which wasn't noticed until after the event.*
- *Miss Z directly engaged with who she was convinced was her solicitor asking for the account details where the money should be sent. Miss Z had never paid the solicitor before and had misplaced the initial bank details the solicitor had sent her.*
- *In Miss Z's own words she felt completely in control of the situation – it was her that was asking for the solicitor's bank details and she'd made arrangements to pay the deposit over two separate days in order to secure the purchase of the property.*

In these circumstances, I'm not satisfied the warning was strong enough to break the spell in the moment. In my view, for the reasons I've previously explained, the warning's primary focus and content is to warn customers about the possibility they're about to fall victim to a scam when they've received unexpected contact, either by phone or email, from a 'genuine organisation' asking them to transfer money. This is not the situation Miss Z found herself in. In her mind she'd received expected contact from a solicitor, within a genuine email chain, asking her to pay the deposit on a property that she was already late paying.

I accept the warning set out that Miss Z should call the 'organisation' directly by telephone, but I'm not persuaded this would hit home to the average consumer when they already think they're liaising with the 'organisation' – in particular when, as I've said, the warning did nothing to explain what email interception looks like in reality. I'm satisfied Miss Z wasn't aware just how sophisticated the methods of posing as a genuine organisation could be.

The common scam examples provided in the warning were too far from the situation Miss Z found herself in to be impactful in the circumstances. In fact, the common scam examples – the nature of which reference unexpected contact – likely offered some reassurance Miss Z wasn't about to fall victim to a scam given the contact was expected and she'd directly asked

for the payment details herself. It's relevant that Miss Z felt completely in control of the situation as the overall tone of the warning indicates you wouldn't be when you're being contacted by a fraudster.

In the circumstances and given how the scam unfolded, I do not think Miss Z acted unreasonably so as to fail to take appropriate action in response to the warnings she was given, particularly when taking into account the warnings limitations.

3. whether taking appropriate action would have had a material impact on preventing the APP Scam which took place?

In this case I've found the warnings were not Effective Warnings given in compliance of SF1(2) and in any event I have found that Miss Z did not disregard the warning by failing to take appropriate steps in the circumstances. Had she taken the suggested steps set out in the warning the scam would have unravelled, but in this case Miss Z did not fail to take appropriate action.

Did Miss Z have a reasonable basis for belief that the payee was the person she was expecting to pay?

I've gone on to think about whether in all the circumstances of the payments, in particular the characteristics of Miss Z and the complexity and sophistication of the scam, Miss Z made the payments without a reasonable basis for believing the payment was legitimate.

Nationwide believes Miss Z didn't, or ought not to have had a reasonable basis for belief that the payments were being sent to her solicitor. This is because:

- *Miss Z's genuine solicitor's emails contained a disclaimer warning its clients about the type of scam Miss Z fell victim to. The disclaimer broadly mirrored the effective warning Nationwide had already provided.*
- *While the change in the solicitor's email address was subtle, Miss Z should've been extra vigilant due to the warnings (from Nationwide and her solicitor) she'd received*
- *Miss Z's email address and password had been compromised in 2018 and this too ought to have put Miss Z on heightened alert*

I'll consider each of Nationwide's points in turn.

<u>Solicitor's disclaimer</u>

I accept Miss Z's genuine solicitor's emails contained a disclaimer which said the following:

"Please note we have been made aware that fraudsters have attempted to persuade a client to send funds to another account. We will never change our bank details and will not provide those details in an open email. Please check with us directly by phone or use the Safebuyer Scheme before sending us any monies as we will not be responsible for any lost funds".

Miss Z says she read this disclaimer when she first saw it, but she did not read it every time the solicitor sent her an email. Instead Miss Z subsequently just read the contents of the email which contained new information. I think this is understandable in the circumstances – after some time repeated disclaimers would likely appear as 'wallpaper' rather than of anything of significance to most recipients.

It's also important to note that the fraudsters emails did not contain the disclaimer. I don't think it's unreasonable that Miss Z didn't notice the absence of the disclaimer – I don't think the absence is remarkable - but this also means that Miss Z wouldn't have read the disclaimer just before making the payment anyway – it seems the fraudster deliberately

removed the disclaimer/didn't include the disclaimer in their email to maximise the chance of the scam succeeding.

Nationwide has said the disclaimer supported and was entirely consistent with the warning it had provided. I accept the disclaimer and the warning contained some similarities, but I'm mindful neither warning set out what this scam looked like in reality when a fraudster tries to persuade someone to transfer them money – importantly this disclaimer, like Nationwide's warning, did nothing to inform the recipient how a fraudster is able to so convincingly pose as the solicitor.

The disclaimer also talks about the fact the solicitor will 'never change our bank details and will not provide those details in an open email', but Miss Z was not under the impression the bank details had changed – she'd simply requested the bank details and had no reason to doubt these were different.

Overall I'm not persuaded the inclusion of the disclaimer means that Miss Z didn't act reasonably, or made the payments without a reasonable basis for belief that the money was being sent to her solicitor.

The change in the solicitor's email address

The change to the solicitor's email address contained an 'i' instead of an 'l'. Nationwide believes Miss Z ought to have been extra vigilant and presumably noticed this, because of the warnings and the disclaimer. I've already explained why I don't think the warnings Nationwide provided were effective, and that the disclaimer didn't explain what email/invoice interception looked like, and so I don't think Miss Z would've closely analysed the email address to check it was exactly the same – particularly as the email from the fraudster was in response to an email she'd sent her solicitor.

I'm satisfied that as far as Miss Z was concerned, she'd received an expected response from her solicitor – it's not realistic for firms to expect customers to look out for tiny discrepancies in an email address, particularly when a firm has not alerted a customer to the possibility of a fraudster posing as a solicitor in the middle of a chain of genuine email correspondence, using the same or a very similar email address.

The compromise of Miss Z's email account and password in 2018

Miss Z says she has evidence that it was not her system that was compromised. Nationwide has said that it was given the solicitor's email address had been changed. Nationwide says it's likely Miss Z didn't change her details following the compromise of her account in 2018 and that even if she had, she ought to have been on 'heightened alert'.

I do not know whether it was the solicitor or Miss Z who had their account compromised at the time of the scam – and I don't intend to make a finding on this. I do not think that Miss Z, or an average customer who did not have a working knowledge about how scams work, or about the events that often proceed them, would've thought about an incident that occurred in 2018, relating to a data breach, when liaising with their solicitor at least a year later. It's unrealistic for Nationwide to think that the average customer would understand that a data breach might lead to a fraudster impersonating a solicitor, in the middle of a genuine chain of emails, asking for money.

And I disagree that Miss Z's actions following the data breach in 2018 has likely led to this scam. There is no evidence to suggest this is 'likely'.

Overall, for the reasons I've set out above, I am not persuaded Miss Z made the payments

without a reasonable basis for belief that she was paying her genuine solicitor.

Final thoughts about reimbursement under the Code

As a final point, I'm currently not satisfied that Nationwide took the time to fully recognise, or find out about, the full circumstances of the scam. It seems that Nationwide only saw the emails between Miss Z and the fraudster and Miss Z and the solicitor after receiving the investigator's view on the complaint. Given the nature of the scam, this is information I'd have expected Nationwide to consider before deciding not to reimburse Miss Z. It seems to me that it's more likely than not Nationwide made the decision not to reimburse Miss Z based on assertion rather than on the evidence that was available to it.

Could Nationwide have done anything else to prevent the scam?

Finally, I've thought about whether, moving away from the CRM Code, Nationwide could've done anything else to prevent Miss Z falling victim to the scam.

The investigator felt that the payments Miss Z were making were out of character and unusual, and that Nationwide ought to have made enquiries about the payments before processing them, to check Miss Z wasn't at risk of financial harm.

Nationwide doesn't agree. It's said, in summary, that:

- *It is not unusual for customers to make occasional legitimate large payments*
- *Miss Z informed Nationwide the payment was for a bill, invoice or property sale which was entirely consistent with her behaviour*
- *To intervene in all situations where a property deposit is being paid would be a significant burden on Nationwide and could cause consumer detriment*
- *There is nothing in the Code to suggest written warnings are insufficient*
- *It doesn't believe its intervention would've made a difference given Miss Z's action after seeing the warnings it provided.*

In this particular case I'm satisfied some of the payments Miss Z made were unusual enough that they ought to have prompted Nationwide to have made enquiries to challenge the purpose of those payments before processing them.

Miss Z made two consecutive payments of £10,000 to a new payee on 7 November. These first two payments were funded by savings Miss Z held with Nationwide and I don't think, in these particular circumstances, that Nationwide ought to have intervened before processing them.

But Miss Z went on to make a further four payments on 11 November to the same payee – three consecutive payments of £10,000 followed by a final payment of £3,500. I think Nationwide ought fairly and reasonably to have contacted Miss Z at the point she attempted to make the first payment of £10,000 the 11 November. This was the third payment to the same payee over a matter of days. At this point Nationwide ought to have been concerned that Miss Z might be at risk of financial harm given a pattern of payments (three £10,000 payments) to a new payee had started to emerge.

Had Nationwide contacted Miss Z asking for information about the purpose of the payment, I'm satisfied Miss Z would've confirmed she was paying the deposit on a new property. In response I'd have expected Nationwide to ask Miss Z how she'd been provided with the bank account details given the prevalence of conveyancing scams (which I'm satisfied Nationwide was aware of at the time). I've no reason to doubt Miss Z wouldn't have told Nationwide she'd been provided with these account details by email, and so in response

Nationwide should've warned Miss Z about the possibility the emails had been intercepted and given Miss Z information about what this type of fraud looked like in reality; encouraging her to call her solicitor to confirm the account details rather than double check them by email.

Had Nationwide done this I'm persuaded it's more likely than not Miss Z would've contacted her solicitor by phone and the scam would have been revealed; preventing Miss Z from losing £33,500.

For clarity, my findings that Nationwide ought to have prevented Miss Z from losing £33,500 have a limited impact on the outcome of this complaint given I have decided Miss Z should've been reimbursed under the provisions of the CRM Code. The impact relates to the interest payable only.

Conclusions

Overall, I'm currently minded to conclude that Nationwide should have reimbursed Miss Z under the provisions of the CRM Code. I'm not satisfied Nationwide established Miss Z ignored effective warnings or that she made the payments without a reasonable basis for belief that she was paying her solicitor. I'm persuaded Miss Z met her requisite level of care.

It's my understanding Nationwide hasn't sought to rely on the other provisions in the Code in declining reimbursement but in any event, I haven't seen anything to suggest Miss Z was grossly negligent.

Further, as I've explained, I think it's more likely than not Nationwide would have prevented Miss Z losing £33,500 had it intervened in the way that I've described above.

In those circumstances, I think Nationwide should now fairly and reasonably compensate Miss Z by refunding her the £53,500 she lost as a result of the scam.

Impact on Miss Z

Finally, I've considered whether Nationwide should pay Miss Z compensation for the distress and inconvenience she's experienced as a result of Nationwide's actions. In considering what's fair compensation, I've specifically thought about the impact of Nationwide's actions, rather than the impact of the crime itself.

I'm persuaded that Nationwide's failure to reimburse, and prevent some of the financial harm suffered, has had a lasting impact on Miss Z. As I explained earlier Miss Z has been left suffering with insomnia and anxiety; and she has been distressed due to the impact on her and her partner's finances and losing their investment property. Whilst I don't doubt Miss Z would have been shaken by what had happened even if Nationwide had done what I have set out it ought to have done, I don't think the impact on Miss Z's health and wellbeing would've been as significant as it has been.

So, for these reasons I think Nationwide should pay Miss Z £400 in compensation.

In my provisional decision I asked both parties to send me any further evidence or arguments that they wanted me to consider by 16 February 2021.

Miss Z accepted my provisional decision and had nothing further to add, and Nationwide has said it is happy to accept my provisional decision in its entirety.

What I've decided – and why

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

As both parties have accepted my provisional decision, I see no reason to depart from my provisional findings, and I remain of the view that this complaint should be upheld for the reasons set out in my provisional decision.

My final decision

I uphold Miss Z's complaint against Nationwide Building Society. I require Nationwide Building Society to:

- refund Miss Z the £53,500 she lost to the scam;
- pay 8% simple interest on the £20,000 from the date Nationwide decided not to refund Miss Z under the CRM Code until the date of settlement
- pay 8% simple interest on the £33,500 from the date of loss (11 November 2019) until the date of settlement
- Pay Miss Z a further £400 for the material distress and inconvenience she experienced.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss Z to accept or reject my decision before 25 March 2021.

Katie Doran
Ombudsman