

The complaint

Ms F complains NewDay Ltd trading as Pulse won't send one-time passcodes by email and about the interest rate she was charged on her account which she says was too high.

What happened

Ms F has a credit card which she took out several years ago – it was a differently branded card when she took it out and wasn't, at the time, managed by NewDay.

In January 2021 Ms F complained to NewDay – who'd been managing her card for several years by then – that she was having problems logging onto her account because she didn't have a mobile phone, or use phones, and so couldn't receive one-time passcodes. Ms F says she's been having problems with NewDay since 2020. For example, she says NewDay unfairly increased the interest rate on her account and then put her on a payment plan.

Ms F's card was going through a re-branding when she complained. In May 2021 she was offered a Pulse card – which is what the card became following the re-branding – which Pulse says she was told she'd have to activate. NewDay says Ms F hasn't activated her new Pulse card, and that her account has been closed as a result.

NewDay investigated Ms F's complaint and said that it had changed its processes for online banking and / or making online payments following the introduction of strong customer authentication rules. It said that it had decided to authenticate its customers using one-time passcodes sent to a mobile phone or through its mobile banking app. It also said that it could send Ms F a one-time passcode to a landline number. In the circumstances, NewDay didn't think it had done anything wrong when it had changed its processes. NewDay also investigated Ms F's complaint that it had unfairly increased the rate of interest on her account. It said that it had charged interest on her account in line with its terms and conditions. In the circumstances, NewDay didn't think it had acted unfairly. Ms F was unhappy with NewDay's responses and so complained to us. She says she stopped using her card and cleared the balance on it after complaining as she was annoyed with NewDay.

One of our investigators looked into Ms F's complaint and said that they didn't think NewDay had acted unfairly by introducing strong customer authentication. Our investigator did, however, think that NewDay had acted unfairly in that none of the methods of authenticating that it offered – all of which involved using phones – were viable alternatives for Ms F as she doesn't use phones. Our investigator recommended £300 in compensation as they thought that this had had a considerable impact on Ms F. Our investigator didn't think NewDay had acted unfairly charging Ms F the interest rate it had done, as it had done so in line with the terms and conditions of the account. Our investigator looked into what happened to Ms F's card following its rebranding, and the circumstances in which her account was closed. Having done so, they thought that Ms F hadn't been able to activate her account because she's been unable to log on.

NewDay didn't agree with our investigator's recommendations. It said that it had opted to send one-time passcodes to their customers' mobile phones and landlines when it rolled strong customer authentication out in January 2021, in order to ensure a smooth transaction.

It said it introduced a process for sending one-time passcodes to their customers via email in mid- October 2021. Ms F's complaint had already been dealt with by then – and it was because of this that she was told that one-time passcodes were only being sent to mobile phones and landlines. NewDay said that Ms F's account had been closed in March 2022 as she didn't activate her new card. Because NewDay didn't agree with our investigator's recommendations, Ms F's complaint was passed onto an ombudsman. As a result, I've been asked to look into her complaint.

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.

Having read the file, I'm satisfied that Ms F doesn't use phones – she genuinely believes that this would put her at risk of fraud and scams – and that she's been very careful to avoid getting Covid-19. I don't necessarily agree with her that she's at risk of fraud and scams for the reasons she gives, but I'm satisfied that she is genuinely fearful of using phones. In the circumstances, I can understand why she prefers to communicate by email rather than by phone. I can also understand why she complained to NewDay when she was told that she'd need to provide a phone number – either a mobile or a landline – so that she'd be able to receive one-time passcodes that she'd need in order to log onto her account or carry out certain transactions online. And I can understand why she wanted NewDay to send one-time passcodes to her email address or allow her to carry on logging into her account the way she'd always done. I'm satisfied that sending one-time passcodes via email wasn't an option NewDay offered at the time.

strong customer authentication

NewDay has told us that it made changes to its processes in order to implement new regulations that came into effect in September 2019 that affected the whole banking sector – namely the Payment Services Regulations 2017 ("PSRs"). Those regulations required payment service providers ("PSPs") to apply strong customer authentication in certain circumstances. Those circumstances are set out in Article 100 of the regulations which says:

"A payment service provider must apply strong customer authentication where a payment service user—

- (a) accesses its payment account online, whether directly or through an account information service provider;
- (b) initiates an electronic payment transaction; or
- (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses."

The FCA gave PSPs until March 2020 to implement strong customer authentication for online banking and has given the e-commerce industry until March 2022 to implement strong customer authentication for online payments. The e-commerce industry includes card issuers, payment firms and online retailers. There was, of course, nothing to stop firms bringing in strong customer authentication sooner than that, if they wanted to do so.

The Payment Services Regulations – which implemented an EU Directive from 2015 commonly known as the revised Payment Services Directive – define "strong customer authentication" as:

“authentication based on the use of two or more elements that are independent, in that the breach of one element does not compromise the reliability of any other element, and designed in such a way as to protect the confidentiality of the authentication data, with the elements falling into two or more of the following categories—

- (a) something known only by the payment service user (“knowledge”);
- (b) something held only by the payment service user (“possession”);
- (c) something inherent to the payment service user (“inherence”);”

In short, strong customer authentication involves, amongst other things, checking that the person accessing a payment account online or initiating an electronic payment is permitted to do so. PSPs have to “authenticate” the person in question using factors based on “knowledge”, “inherence” or “possession” and must use at least two independent factors when doing so. They can’t, for example, check using only “knowledge” based factors, but they can check using one or more “knowledge” based factors and one or more “possession” based factors. Ms F is unhappy that NewDay changed its processes and unhappy that the changes involved having to use a phone.

NewDay’s approach to implementing strong customer authentication

I don’t think it was unfair or unreasonable of NewDay to implement strong customer authentication – it’s an important measure to help combat fraud. In this particular case, I don’t, therefore, think it was unfair or unreasonable of NewDay to say to Ms F that she wouldn’t be able to log into her account using her user ID and memorable data only as that wouldn’t constitute strong customer authentication – this would be authentication based on one rather than two factors. I can also understand why NewDay decided that it would send one-time passcodes to its customers’ mobile phones and landlines when it first rolled out strong customer authentication – in January 2021 – as I accept those were the main methods by which its customers got into contact. I do, however, agree with our investigator that NewDay needed and needs to offer alternative ways of authenticating that are viable for customers like Ms F. I’d like to explain what the FCA has said about strong customer authentication and its expectations first before saying what I think that means in this case.

What has the FCA said about strong customer authentication and its expectations?

The Financial Conduct Authority (the “FCA”) has published several papers about strong customer authentication and its expectations and it has written to firms about this too. In a paper published in June 2019 – “Payment Services and Electronic Money – Our Approach” – the FCA described its approach to the PSRs and payment services and e-money related rules in its Handbook. In paragraph 20.21 of its paper the FCA said:

“We encourage firms to consider the impact of strong customer authentication solutions on different groups of customers, in particular those with protected characteristics, as part of the design process. Additionally, it may be necessary for a PSP [Payment Service Provider] to provide different methods of authentication, to comply with their obligation to apply strong customer authentication in line with regulation 100 of the PSRs 2017. For example, not all payment service users will possess a mobile phone or smart phone and payments may be made in areas without mobile phone reception. PSPs must provide a viable means to strongly authenticate customers in these situations.”

The FCA has, in my opinion, made it clear in its paper and elsewhere that businesses shouldn’t rely on mobile phones alone to authenticate their customers and should provide

viable alternatives for different groups of customers. The FCA has, in my opinion, also made it clear in this paper and elsewhere that this includes people who don't possess a mobile phone or a smart phone and not just those who can't use one. The FCA has talked, for example, about managing the potentially negative impact of strong customer authentication on different groups of customers "particularly the vulnerable, the less digitally engaged or located in areas with limited digital access". And the FCA has also talked about the need for firms to develop strong customer authentication "solutions that work for all groups of consumers" and has said that this means they "may need to provide several different authentication methods for your customers".

why is Ms F complaining?

Ms F is complaining that NewDay told her that it couldn't send one-time passcodes via email and that she'd have to provide a mobile phone or landline number if she wanted to receive one-time passcodes in order to log into her account online and make certain payments. That's because she doesn't use phones. Before complaining and Covid, Ms F says she used a device belonging to her daughter to log into her account. Ms F says her daughter now uses this device so it's no longer convenient for her to do so, but she does have access to another device that allows her to go online when she needs to. She wanted NewDay to either send one-time passcodes via email or allow her to carry on logging on the way she always had done – in other words, allow her to log on using her user ID and memorable data. She says she wants to be able to access her account over the internet and not via an app as she doesn't have space on her device for apps. So she wasn't happy when NewDay sent her an email with a link to its app.

should NewDay have done more for Ms F?

I've already said why I don't think it was unfair or unreasonable of NewDay to say Ms F couldn't log on using her user ID and memorable data alone. This wouldn't be strong customer authentication. So the main issue I have to decide is whether or not NewDay ought to have offered Ms F other ways of authenticating that didn't involve phones.

The FCA's guidance says that businesses should offer customers alternative ways of authenticating that don't involve mobile phones. I agree with NewDay that it did offer an alternative – it offered to send one-time passcodes to landlines too. The FCA guidance, however, also makes it clear that businesses should consider the impact on different groups of customers as part of the design process and that it might be necessary to provide different methods of authenticating. In Ms F's case, I agree with our investigator that NewDay could and should have done more to help as it's clear she was struggling with the options it had given as they all involved phones of one sort or another.

NewDay says that since Ms F complained it has decided to send one-time passcodes via email too. In other words, NewDay has introduced an alternative that ought to work for Ms F. In order to get a one-time passcode sent via email, however, NewDay has told us that Ms F would have to phone its customer service department. That's despite Ms F making it clear that she doesn't use phones.

I'm satisfied, given everything that I've said, that NewDay could and should have done more for Ms F and that she had problems accessing her account because NewDay didn't offer her an alternative way of authenticating that was viable for her. Ms F has told us that she cleared the balance on her card and stopped using it after she complained. She's also told us that the card is no longer a joy to use. In the circumstances, given that NewDay says her account has been closed because her new card wasn't activated, I agree that compensation is the appropriate remedy in this case.

Putting things right

I agree with our investigation, given the impact NewDay not offering an alternative way of authenticating that is viable for Ms F, that an award of £300 is fair in this case. So that's the amount I'm going to require NewDay to pay Ms F in full and final settlement of her complaint.

My final decision

My final decision is that I require NewDay Ltd to pay Ms F £300 in compensation in full and final settlement of her complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms F to accept or reject my decision before 26 October 2022.

Nicolas Atkinson
Ombudsman