DRN-3295599

The complaint

Ms W complains Vanquis Bank Limited didn't offer her an alternative way of authenticating that didn't involve phones when it implemented strong customer authentication. Ms W also complains Vanquis Bank Limited didn't remove an old number or send her statements in the meantime so she could check her account making it harder for her to manage her account.

What happened

Ms W opened a Vanquis account several years ago in part to help build her credit rating. She's had difficulties with her finances in the past and has developed a system for managing her finances because of this that worked well. The system is important for her as she has disabilities that affect her memory and her mental health.

In October 2020 Ms W contacted Vanquis to say she was having difficulties managing her accounts online – which is an important part of her system – because she wasn't able to receive one-time passcodes as she didn't have a mobile phone or a landline she could use for this purpose. In the meantime, she asked Vanquis to send her statements so she could check her account. She wanted to know why she couldn't carry on receiving one-time passcodes to an email address. Ms W also asked Vanquis to remove an old mobile number from its records saying that she was worried what it might be sending to that number.

Vanquis looked into Ms W's complaint and said that it had chosen to authenticate its customers by sending one-time passcodes to mobiles or landlines – and that it could no longer send one-time passcodes to an email address as that wasn't strong customer authentication compliant. Vanquis removed the old mobile number from Ms W's records and offered her £50 in compensation as it accepted that there had been a delay in doing so. Vanquis said Ms W could also use its telephone banking service.

Ms W was unhappy with Vanquis's response for a number of reasons – for example, it kept on explaining to her how to use its app (which she couldn't as the whole point of her complaint was that she didn't have a mobile) rather than how to access its website. In relation to the options that Vanquis offered – namely sending a one-time passcode to a mobile or a landline – Ms W said that the FCA had issued guidance saying firms should be offering alternative ways of authenticating that didn't involve phones and that in any event Vanquis relying on phones only also meant that it was discriminating against her. She complained to us.

One of our investigators looked into Ms W's complaint and said that they didn't think Vanquis had treated her fairly. They recommended that Vanquis pay her £200 in compensation and offer her an alternative way of authenticating that didn't involve phones. Vanquis didn't accept our investigator's recommendations, saying that it had complied with strong customer authentication regulations by offering customers without a mobile an alternative, namely sending one-time passcodes to their landline. Vanquis asked for an ombudsman to look into Ms W's complaint. So, that's what I've done.

I issued a provisional decision in October 2022 saying that I agreed with our investigator that Vanquis ought to offer Ms W an alternative way of authenticating that doesn't involve

phones. I said that this might include one of the alternatives UK Finance had suggested in papers it has published on implementing strong customer authentication in relation to vulnerable customers in particular. I also said the I thought Vanquis should pay Ms W £350 in compensation for the distress and inconvenience it had caused her. Both sides were invited to reply to my provisional decision and both sides did.

Ms W was very disappointed with my decision and very disappointed that I hadn't said anything about late fees she believed she'd been charged and adverse information that she believed Vanquis had recorded against her given the problems she's had managing her account ever since Vanquis made changes. She also wanted me to ask Vanquis to remove the landline number it had on its system for her. Vanquis didn't agree with my decision either. It said that it had no choice but to implement strong customer authentication and that the alternatives UK Finance had suggested breached strong customer authentication regulations as did other options we'd suggested. Vanquis also said that offering Ms W another method of authentication wasn't achievable or proportionate particularly as she, according to Vanquis, "chooses" not to use a mobile phone or a landline. Finally, Vanquis said it had only charged one late fee since Ms W had complained – in September 2022 – and that it hadn't recorded any adverse information against her.

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.

Background

As I mentioned in my provisional decision, the majority of the facts in this complaint aren't in dispute. It is, however, helpful to say a bit about Ms W's background and the way she manages her finances. So, I'm going to do so again here. It explains why Ms W is a vulnerable customer and why I consider Vanquis's response to my provisional decision unhelpful and disappointing.

Ms W had been a customer of Vanquis for many years before she complained about the way it had gone about implementing strong customer authentication and has had credit for many years. In the past, and in particular before she started using online banking regularly, it's clear that Ms W had problems managing her finances given her memory problems. It's clear that the ability to use online banking – which she can access when she needs to (particularly when she remembers something late at night that she might forget by the following morning) and which allows her to see what's happening to her accounts (she finds it easier to see information than listen to information because she's a visual person) – has been invaluable in her getting on top of her finances. It's also clear she has been able to rebuild her credit score in recent years – a positive that Ms W is proud of, and rightly so. Indeed, this was one of the reasons why she was originally attracted to Vanquis as taking out a credit card with them was one of the steps she took to help rebuilding her credit score.

Ms W is able to use a mobile phone, but she doesn't have her own personal mobile phone. She has a work mobile but can't use this mobile for her own personal business. Her partner has a mobile phone too, which she uses from time to time, but they work away for long periods of time, so this isn't an option she can rely on. She used to have a landline, but she hasn't replaced the handset ever since it broke given the volume of scam calls she used to receive. And finally, her neighbour has a landline which she has sometimes borrowed, but this is not an option she wants to or can rely on. In short, she doesn't have regular access to her own phone – she's a visual person in any event. In the circumstances, given what I've said about how she manages her finances and the reliance she places on being able to see rather than hear information, I can understand why she told Vanquis she didn't want to use

its telephone banking – she's a visual rather than verbal person – and why she was worried that she might not be able to access her online banking easily going forwards given Vanquis's reliance on phones to authenticate its customers.

strong customer authentication

As I've just mentioned, Ms W was happy with the way her online banking operated until Vanquis introduced changes to the way its online banking worked. Those changes involved, amongst other things, sending a one-time passcode to their customers' mobile phone or landline so that they could authenticate themselves.

Vanquis 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 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 gave 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.

Vanquis’s approach to implementing strong customer authentication

As I said in my provisional decision, I don’t think it was unfair or unreasonable of Vanquis to implement strong customer authentication – it’s an important measure to help combat fraud. Nor do I think it was unfair or unreasonable of Vanquis to use one-time passcodes to help prove “possession”. But both the FCA guidance – which I’m about to say more about – and the papers UK Finance have published also say it’s important that vulnerable people in particular aren’t excluded from online banking and shopping as this can be just as harmful as the fraud strong customer authentication is designed to combat.

Ms W doesn’t disagree with strong customer authentication – but she believes that Vanquis hasn’t acted in line with FCA guidance because it has only offered methods of authentication that involve phones. She believes that this is discriminatory as well as breaching the FCA’s guidance. In the circumstances, as I did in my provisional decision, I think it would be helpful to explain what the FCA has said about strong customer authentication and its expectations.

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 W complaining?

As I've already mentioned, Ms W isn't complaining about the fact that she's unable to authenticate because she can't use a mobile phone – she can use a mobile phone and does use one. Her complaint is about the fact that Vanquis doesn't offer ways of authenticating that don't involve phones because she doesn't have regular access to her own phone – one of the mobiles she uses is a work phone (so not one she wants to use for personal matters or can use for personal matters) and the other mobile she uses is her partner's (who is often away working for long periods of time) – and in any event she's a visual person. That means I have to decide whether or not Vanquis ought to have been providing alternatives that didn't involve phones before Ms W complained and whether or not what it has done in all the circumstances is fair and reasonable. At this stage I think it's worth saying that I don't agree with Vanquis that Ms W "chooses" not to use a mobile phone or a landline. Ms W relies on online banking because she has disabilities that affect her memory and her mental health and because she's a visual person. That's one of the reasons why she doesn't find it easy, for example, to manage her account using telephone banking – it's not visual. Vanquis' suggestion, therefore, that she "chooses" not to use a mobile phone or a landline – in other "chooses" not to use non-visual channels – is not only disappointing but also concerning as it suggests it doesn't have a good and sympathetic understanding of vulnerability.

Should Vanquis have done more for Ms W?

The FCA guidance doesn't, in my opinion, say that businesses shouldn't only offer alternatives that allow authentication by phone. The guidance talks about mobile phones and smart phones, rather than landlines, and the importance of providing different methods of authentication that don't involve mobile phones or smart phones. A landline could, therefore, be seen as an alternative method of authenticating, and for many people who don't own or can't use a mobile phone or a smart phone, it might well be an option that works well. Nor do I necessarily agree with Ms W that Vanquis's approach in itself was discriminatory. I do, however, agree that in her case Vanquis could have done more to help as it should have been clear from her complaint that Ms W was a vulnerable customer who relies heavily on being able to manage her account online and a visual person too.

As I mentioned in my provisional decision, UK Finance has published a paper – as part of an initiative to help the industry come up with strong customer authentication solutions, in particular for vulnerable customers – which identifies a number of options (including authentication via email) that businesses have been encouraged to consider. That paper says that firms might even consider using one factor authentication for vulnerable customers for whom there are few, if any options, that might work or exempting them entirely. The FCA has encouraged firms to get involved in UK Finance's initiative. Given that I mentioned all of this in my provisional decision, it is disappointing that Vanquis has suggested that the options UK Finance have suggested don't comply with strong customer authentication regulations and that Vanquis hasn't appreciated that not being able to access online banking and shopping can be just as harmful as the fraud strong customer authentication is designed to combat. In its response Vanquis suggested that in the future it might consider terminating its relationship with a customer if the limited channels it offered didn't work for that customer as a way to prevent harm. That was a very disappointing response too.

It's clear from Ms W's complaint that she was particularly worried that she'd made late payments and had adverse information recorded against her because she's not been able to manage her Vanquis card the way she did before it made changes. I can see why that would be a real worry given the hard work she's done rebuilding her credit score. So, I hope it's reassuring for her to know that Vanquis has only charged her one late fee – in September 2022 – and that it hasn't recorded any adverse information against her since she brought her complaint. That's because she's paid off her balance in full every month – albeit late in

September 2022 – likely because of the statements she was receiving.

Putting things right

In my provisional decision I said that I agreed with our investigator that Vanquis ought to offer Ms W an alternative way of authenticating that doesn't involve phones. I also said that this might include one of the alternatives UK Finance had suggested. Given that Vanquis has made it clear it isn't willing to offer an alternative – despite everything the FCA and UK Finance has said – I'm going to increase the compensation I awarded to Ms W to reflect the fact that her Vanquis credit card is not as manageable as it used to be. I'm also going to require Vanquis to refund the late fee it applied in September 2022 as I'm satisfied Ms W wouldn't have paid late had she been able to rely on the system she's developed over time. I consider £500 in compensation to be a more adequate remedy. I appreciate that compensation wasn't what Ms W was looking for and would understand if she decides she no longer wishes to be a Vanquis customer given its response to this complaint – at least if she did so she would have already achieved her aim of rebuilding her credit score. In the meantime, Vanquis ought to continue sending Ms W paper statements at no charge to help mitigate the problems the changes it has made will cause Ms W when it comes to managing her account.

My final decision

My final decision is that I require Vanquis Bank Limited to pay Ms W £500 in compensation and to refund the late fee it charged her in September 2022.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms W to accept or reject my decision before 21 February 2023.

Nicolas Atkinson
Ombudsman