DRN-3563608

The complaint

A complains that PrePay Technologies Limited t/a Counting Up failed to refund several transactions that they didn't recognise from their account. A also complain a payment was delayed and Counting Up were rude in their communications.

What happened

The background to this complaint has already been explained in some detail, but, for completeness, I'll replicate the full provisional decision here which sets out the details of the complaint and my initial thoughts on it.

A held an account with Counting Up and when they checked their mobile app they noticed the account had almost been emptied overnight. A contacted Counting Up about this who confirmed they'd registered a change on the account to allow another device to have access to it.

A told Counting Up that they hadn't made any of these changes or transferred or spent the funds from the account. Counting Up looked into what had happened and told A that they'd sent emails notifying A about the change to the address that A had registered with them. It was this email that allowed the changes to be made to the account. A said they hadn't received them and couldn't find them within their email system.

Counting Up told A that in order for a payment to be made from the account, someone would need access to A's device and be able to receive a message to verify the transfer. A confirmed to Counting Up that no one else had access to their device.

A told Counting Up that they'd received a message from them about a new payee that was being set up and had clicked on a link to say "no" to this. Counting Up investigated the issue and the next morning asked A to check that all their details were correct, including the registered phone number. When A looked at their app, the phone number had been changed from the one that A had originally registered with Counting Up. A changed the number back and also changed the password on their email account on the advice of Counting Up.

Counting Up contacted the banks responsible for receiving the transfers from A's account and secured £4,160.35 for eventual return to A. Counting Up declined to refund the remaining money and told A they believed they were in breach of their terms and conditions. This was because A had allowed their email address to be compromised, which in turn allowed an unauthorised third party to gain access to the Counting Up app and take over the account.
A told Counting Up that they weren't aware their email had been compromised, they said that the operator of the email had confirmed it hadn't been "hacked" and A's own anti intrusion software hadn't detected anything on their mobile phone that used the app. Counting Up told A that if the email wasn't hacked, then the only other way to make the transfers was to have access to the app on A's mobile phone. A contacted Counting Up a week or so after the original event and said someone was trying to register a new device which wasn't them. Counting Up prevented any new devices for being registered

for a period of time.

A complained to Counting Up about the loss of their funds, how they'd been dealt with and that there had been a delay when their funds were returned. A also believed that Counting Up's systems had been breached. Counting Up didn't change their opinion and declined to refund A, apart from returning the recovered funds. Counting Up held A liable and said:

"Unfortunately, we are not able to refund the remaining missing sums. This is because Countingup is not liable for those transactions under 10.5.1 of our Terms and Conditions and 10.6.
This is because once they gained access to your email address, a 3rd party was able to access either your card details or your Countingup up app in order to set up the app on their own device.
As such, either access to the card itself or to your device (and therefore, the Countingup app) was not made secure, which constitutes gross negligence under our Terms."

A was unhappy with how Counting Up had dealt with their losses and brought their complaint to the Financial Ombudsman Service for an independent review. It was looked into by one of our investigators who asked for evidence from both parties. A explained that no one else had access to either their mobile phone or laptop, they were password protected and had anti-intrusion software fitted. A said no one else had been told the passwords to access these devices or the Counting Up app. A confirmed that no one had approached them about their account or tried to obtain details about it. A confirmed they'd received a text message from Counting Up about a new payee and had replied "no" to this because they didn't recognise setting up any new payee. A confirmed they'd notified the police about the fraud.

A later explained that prior to the transactions happening, they'd noticed an email arriving in their inbox but then couldn't locate it. A said they'd received a message via a popular messaging app that contained a video which had been briefly viewed but later thought was unusual.

Counting Up provided a timeline of the events including their contact with A when they were notified about the losses and details of the process needed to add a new device to the account. Counting Up told A they'd sent an email to the registered address held for A and because they'd received an appropriate response to it, which included details (last four digits) from A's Mastercard, they'd made changes to the account.

Counting Up explained that the transfers couldn't have happened without access to A's device and knowledge of the password. New bank transfers also triggered a text message which needed to be verified before the transfers could happen. One of the disputed payments was also made with A's Mastercard details. Counting Up said these details weren't available in their app and could only be found on the physical card. Counting Up explained they'd asked A to change their email account password and to check their details on their Counting Up account. It was later found that the mobile phone number had been changed.

Counting Up believed they'd acted appropriately when they'd dealt with A and recovered their money in a timely manner.

Our investigator thought that A hadn't authorised the transactions and had been the

victim of a technical "hack" on his phone as a result of opening a video file which led to the compromise of A's Counting Up account. Our investigator didn't think that A had been grossly negligent and upheld A's complaint.

Counting Up disagreed with the investigator's outcome and questioned the "hack", they hadn't seen any evidence of this and believed it was speculation. They didn't believe this was the reason for the loss of A's money, but they accepted that A "….*may not have authorised the transactions*".

Counting Up didn't think their position had been correctly represented because the investigator had only relied on the "gross negligence" aspect of the Payment Service Regulations and hadn't considered the terms and conditions used by Counting Up to deny A the refund. Counting Up considered their terms and conditions went "*beyond gross negligence*". They said:

"(The investigator) appears to focus their reasoning on "gross negligence" over the correlation between Clause 10 of Counting Ltd's Terms and Conditions and 72 (1) of the Payment Services Regulations 2017"

They continued to question how the Mastercard disputed transaction(s) could have taken place because there was no explanation how the card details could have been obtained by the fraudster. Counting Up asked for a further review of the complaint which has been passed to me for a decision.

I've issued two provisional decisions for this complaint, the first of which said:

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

The main thrust of Counting Up's case is that A breached their terms and conditions. But before I can consider that, I need to satisfy myself regarding the question of authorisation.

Authorisation

Counting Up said in their initial response to the Financial Ombudsman that A "….may not have authorised the transactions". In a later response they said it was unknown to them if A authorised the transactions or not.

So, the question of authorisation hasn't yet been sufficiently considered. I've previously asked Counting Up for evidence of authentication related to all the disputed transactions but have yet to receive a full response to this request.

The relevant law surrounding authorisations is the Payment Service Regulations 2017 (PSRs). The basic position is that Counting Up can hold A liable for the disputed payments if the evidence suggests that it's more likely than not that they made them or authorised them.

Authorisation is made up of two parts. Authentication and consent. Authentication is usually referred to as the technical evidence and in this case I haven't yet seen sufficient evidence to satisfy myself that the transactions were authenticated. Without that evidence, that makes it very difficult for me to say that they were authorised in the way the rules say.

Because A have denied authorising the disputed transactions and Counting Up have yet to show they were properly authenticated, that would usually mean Counting Up are liable to make a refund to A.

Whilst I appreciate that Counting Up have focused on the fact that they believe A has been 'grossly negligent' in how these payments were made – it remains that the regulations here explain that it's for a payment service provider to prove that a payment transaction was authenticated and accurately recorded. So, viewed purely on the basis of whether these transactions were authorised, I'd be thinking of upholding the disputed transaction aspect of this complaint based on the lack of authentication data. This is relevant here, based on what I'll go onto say about the basis for Counting Up's refusal to refund A.

Gross negligence

Counting Up have relied on their terms and conditions to deny A a refund. Essentially, they make the case that because their terms and conditions go "beyond gross negligence", A have breached them because their email system was "hacked".

Counting Up's terms state:

"10.5 You will be liable for all unauthorised transactions that arise from the use of a lost or stolen Card or Account security information or the misappropriation of the Card if you fail to:
10.5.1 keep the Card and/or security features of the Card and Account Safe…"

Counting Up argue that clause 10.5.1 allows them to deny A a refund because they believe this term covers the circumstances of this complaint, i.e. that if A's account was "hacked" then this means it wasn't kept safe and therefore in breach of this term.

Counting Up have quoted parts of S 72 (1) of the Payment Service Regulations in their submission, specifically:

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

(a)use the payment instrument in accordance with the terms and conditions governing its issue and use;

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

(a) use the payment instrument in accordance with the terms and conditions governing its issue and use"

S 72 contains further parts, so I've replicated the complete section here:

*"**Obligations of the payment service user in relation to payment instruments and personalised security credentials***

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

(a)use the payment instrument in accordance with the terms and conditions governing its issue and use; and

(b)notify the payment service provider in the agreed manner and without undue delay on

becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

(2) Paragraph (1)(a) applies only in relation to terms and conditions that are objective, non-discriminatory and proportionate.

(3) The payment service user must take all reasonable steps to keep safe personalised security credentials relating to a payment instrument or an account information service."

Whilst it's accepted that account users must follow the terms and conditions governing the use of a payment instrument (which includes the use of an app), those terms must be objective, non-discriminatory and proportionate.

This is reinforced by the FCA's approach document 'Payment Services and Electronic Money' which says (8.175 on page 120):

The customer is obligated by the PSRs 2017 to abide by the terms and conditions for the use of the payment instrument. A customer does not, however, need to abide by any term unless it is objective, non-discriminatory and proportionate. We would consider terms and conditions which, for example, require customers to open and destroy a PIN notification immediately or which prohibit customers from writing down or recording their PIN in any form not to be permitted.

The FCA expands on that in 8.179:

The PSRs 2017 also obligate the customer to take all reasonable steps to keep the personalised security credentials relating to a payment instrument or an account information service safe. This would include the PIN or password for the instrument or other piece of information known only to the issuing PSP and the customer. It does not include, for example, a credit card number itself, as this would be known to any business where the card was used.

8.180 What constitutes reasonable steps will depend on the circumstances, but PSPs must say what steps they expect customers to take in their pre-contract disclosure information …

So here, Counting Up's use of "beyond gross negligence" to describe their terms and conditions isn't something contained in the PSRs. The specific term they rely on is quite generalised, but I'm not persuaded their interpretation of this term and the wider regulations and guidance has led to a fair outcome here.

In saying this, I've considered that The FCA says:

"…we interpret "gross negligence" to be a higher than the standard negligence under common law. The customer needs to have shown a ***very significant degree of carelessness." (****Payment Services and Electronic Money: Our Approach).*

So, to prove that A were grossly negligent, Counting Up have to show that they acted in such a way as to be so careless that they have met the above interpretation of this term. If a third party was responsible for these disputed transactions without the knowledge of A, and they (A) hadn't done anything to obviously facilitate that "hack" or had been legitimately tricked into it, then I currently find it difficult to accept that it meets the definition.

I appreciate that the introduction of a possible "hack" through a message opened by A was a surprise to Counting Up and I've not seen any evidence that clearly supports this as the

reason for how the account was compromised here. I can't say with any certainty what happened at this point, but A have been consistent in their version of the events and can't offer any explanation other than it wasn't them that carried out the transfers or used the card to make a payment.

If Counting Up consider that A were grossly negligent, the PSRs require them to provide supporting evidence to the payer (A) that demonstrates this:
S 75 (4) says:

"If a payment service provider, including a payment initiation service provider where appropriate, claims that a payer acted fraudulently or failed with intent or gross negligence to comply with regulation 72, the payment service provider must provide supporting evidence to the payer"

So, what the regulations require is that Counting Up demonstrate to A with evidence, their belief that they were grossly negligent. What appears to be the case here is that Counting Up are relying on an absence of evidence to show that A were grossly negligent - because of a non-specific compromise of A's electronic systems. I think it would be difficult for Counting Up to satisfy S75 on that basis. Put simply, gross negligence must be based on something rather than nothing.

I've looked at the basis on which Counting Up say that A has been grossly negligent here. But for the reasons given above, I'm not persuaded by their current argument as to why or how A has been grossly negligent.

10.6 T&C

Counting Up also relied on this section of their terms to deny A any refund. Counting Up weren't specific about which parts of this section they were referring to as it covers aspects of authorisation and app/device/information security, including the use of their card in an Automated Teller Machine. So, as it's unclear what they were referring to and I've already considered the issues of authorisation and gross negligence, I don't intend to comment further about this. If Counting Up wish to clarify any points then I'll be happy to consider them.

So, it falls to Counting Up to show the payments were either authorised by A or they were grossly negligent. My current thinking is that because Counting Up haven't demonstrated that the payments were authenticated, I'm intending to uphold this complaint on that basis.

But, if evidence is produced that demonstrates proper authentication, including the receipt of the email verifying the new device, I'll then consider whether it was more likely than not that A authorised the payments.

Security

System security is a feature of each party's positions who've both claimed their respective systems were operating properly at the time. A stated that their email provider and anti intrusion software reported their systems were working ok and Counting Up stated " (Counting Up) did not partake, actively or passively, in the compromising of A's credentials."

So far, neither party have supplied evidence to support these claims which makes it difficult for me to make any assessment about it.

The PSRs (S75) state… "it is for the payment service provider to prove that the payment transaction was … not affected by a technical breakdown or some other deficiency in the

service provided by the payment service provider."

I don't think it's unreasonable for Counting Up to demonstrate that their systems were working properly as they've specifically defended this aspect of the complaint and there's an obligation under the PSRs to do so. I appreciate there's an element of "proving a negative" here, but I think it would be helpful to see that their systems were operating properly at the time of A's loss.

Similarly, A haven't yet provided evidence of their own claims about the security of their systems (email integrity and phone security report), so I think in the interests of a fair and reasonable outcome, evidence should be, where available, provided to support this.

Card payment data

Counting Up provided authentication data for one Mastercard transaction, which I've had chance to review. Counting Up have stated that the CVV (three-digit security number) would have likely been required to make the transaction and that information is only available from the physical card. There's no evidence that the CVV was entered when the payment was made, so I'm not convinced this point is relevant.

Return of funds

A complained that the recovered funds took too long to be repaid into their account. I haven't seen evidence of how long this took but Counting Up supplied evidence that they'd requested it and informed A that they'd chased it up. I appreciate that there's a link between the companies, but it's the responsibility of the receiving bank to return the funds and to an extent, Counting Up have little control over this. From the evidence I've been able to consider, I'm currently intending not to uphold this aspect of the complaint.

Counting Up's treatment of A

A also complained that Counting Up were rude when they communicated with them. I've read through all the correspondence between A and Counting Up that has been supplied by both parties and couldn't see that they'd been rude to A. Counting Up responded to A's questions and chased up the receiving bank's once A had notified them about the fraud. I don't think the correspondence between them shows that Counting Up were rude to A and I'm currently thinking that I won't uphold this aspect of the complaint.

Summary

Because authentication hasn't been satisfactorily dealt with, I'm currently intending to uphold A's complaint concerning the disputed transactions and to instruct Counting Up to refund them with simple interest at 8% added from the date of loss to the date it's repaid. I'm currently intending not to uphold the other aspects of the complaint. But, if the question of authentication is satisfactorily answered, I'll then consider the broader question of authorisation. Depending on the outcome of that, I'll then need to decide if gross negligence is relevant to the outcome of the complaint.

I invited A and Counting Up to give me any more evidence and information they wanted me to consider before issuing my final decision. A didn't respond and Counting Up provided additional evidence concerning the operation of their systems and authentication data about the disputed payments.

I then issued a second provisional based on receipt of the authentication data and addressed the issue of authorisation.

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

As mentioned in my first provisional decision, I hadn't been able to assess the issue of authorisation because evidence hadn't been provided at that point. Counting Up have since sent me that evidence so I can now address this aspect of the complaint.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Counting Up can hold A liable for the disputed payments if the evidence suggests that it's more likely than not that they made them or authorised them.

Counting Up can only refuse to refund unauthorised payments if it can prove A authorised the transactions but Counting Up cannot say that the use of the card and banking app conclusively proves that the payments were authorised.

This is in line with the FCA's position, as outlined in its document setting out its role under the Payment Services Regulations 2017. The FCA says:

To avoid doubt, it is not sufficient for the PSP to assert that the customer "must have" divulged the personalised security features of the payment instrument, and to effectively require the customer to prove that he did not. The burden of proof lies with the PSP and if a claim that a transaction is unauthorised is rejected, the rejection must be supported by sufficient evidence to prove that the customer is guilty of fraud, gross negligence or intentional breach and the reason for the rejection must be explained to the customer.

Unless Counting Up can show that consent has been given, it has no authority to make the payment or to debit A's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to A.

Because the transactions were properly authenticated by the payment tools issued to A, I'm satisfied that Counting Up had the appropriate instructions with which to carry out the transactions. But, I'll now need to consider if sufficient evidence has been provided to show that A consented to the transactions.

Part of the evidence supplied by Counting Up relates to three devices registered to A's account, including IP address data about them.

Note: IP addresses are a means to identify physical locations that online transactions are connected to and can be the actual physical location or other locations connected to the provider of the data services.

Counting Up have explained that in order to register a new device, an email is sent to the registered address for the account and details from the Mastercard are required to be entered to confirm the action. Counting Up have provided evidence that they sent emails to A's registered email address. The new device was registered because the correct process was followed, including the details taken from the Mastercard. Once the new device was registered, it was used to set up new payees and send funds to other accounts.

The details from the Mastercard aren't contained in the app, so it would seem that access to the physical card was required, or knowledge of the details contained on it plus access to A's email before the new device was registered. A have explained that their email account provider confirmed that the account wasn't compromised, although A have also said there was an email (from Counting Up) that later couldn't be found. Counting Up have also

supplied evidence that their own systems were operating normally at the time of the disputed transactions.

Data shows that three devices were registered to the account. A explained they only used one device, but it wasn't responsible for setting up the new payees and transferring funds to different bank accounts. A second device was used to complete all these steps, which again needed specific security details known only to A. There was also a third device which was briefly registered on the account but wasn't used to make any disputed transactions. A confirmed they didn't pass security details to anyone else. So, it's difficult to think of a plausible scenario where an unauthorised third party could complete all the steps necessary to register a new device/set up new payees and make several disputed transactions without access to A's email and knowledge of details known only to A.

A mentioned opening a video message via a messaging platform which our investigator thought could be responsible for the later compromise of A's account. Some evidence of a general weakness in the messaging platform was produced which explained how such compromises could work. But, there's no evidence of any compromise (hack) of A's system, which was backed up by their email providers confirmation. Of course, it's possible that such technical compromises of A's systems could have taken place without it being evidenced, but I don't think it's the likely explanation.

In order to complete the registration of a new device, the Mastercard details would be required which aren't available on Counting Up's app – so it's likely whoever set up the new device had access to the Mastercard.

I've also examined IP address data linked to the three devices using the app. A's regular device and the new device use the same broadband provider, although the bulk of activity took place over different IP addresses. But, A's regular device logged on from the same IP address used by the new device. This took place the same day as the disputed transactions. This would indicate that whoever made the disputed transactions did so from the same location that A were also logged on from. It seems unlikely that an unidentified third party would be using the same location as A on the day the disputed transactions were made.

I've also considered the single disputed transaction that used the Mastercard. The user of the card needed to either have the physical card or obtain the card number and other relevant security details. A didn't lose the card and I've already made a finding that I don't think a technical "hack" was responsible for acquiring the details of it. I think that it's more likely than not that A were responsible for using the card or allowing someone else to use it.

So, taking everything into account, my current thinking is I think it's more likely than not that A were responsible for making these disputed transactions. Whilst I'm sure A will disagree with me, there's currently no plausible explanation how an unauthorised third party could obtain access to A's email system, acquire the Mastercard details from the card and use the same IP address as A. Because I've made a finding about authorisation, I don't currently need to consider whether A breached their terms and conditions or the issue of gross negligence.

I see no reason to change my first provisional decision regarding the other aspects of A's complaint.

My provisional decision

My current thinking is that I do not intend to uphold this complaint.

I invited A and Counting Up to give me any more evidence and information they wanted me to consider before issuing my final decision. Counting Up didn't have anything further to add and A provided information concerning contact with his mobile phone supplier and comments about the IP address data. A also provided screenshots from his email provider relating to possible changes with their account.

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.

A provided an analysis of the IP data that Counting Up had supplied and information from their mobile phone and email supplier. A have argued that there's evidence of third parties attempting to access their mobile phone and email account. They also believe there's no evidence of matching IP address data.

I've looked at the information A provided in relation to the information from their mobile phone and email provider, which consists of text messages dated after the disputed transactions took place. Both sets of texts relate to attempts to change information about their accounts. A's mobile phone provider asks A to bring identity information in following their enquiry. It goes on to say that once identity has been confirmed – access to the account can be granted. A replied to the text stating that someone has been trying to impersonate them.

The text seems to indicate someone contacted the mobile phone supplier – but they weren't able to gain any access to the account. This text is dated after the disputed transactions had already taken took place and also confirms that no one was able to access it because they couldn't satisfy the provider's security requirements.

Regarding the text from A's email provider, this also relates to attempts to change information about the account, specifically the mobile phone number. This also happened after the disputed transactions had already taken place.

So, whilst A may have been subject at some point to an attempt to gain access to their accounts, these attempts happened following the movement of the funds out of the account. If, as A state, that third parties were responsible for the disputed transactions, I can't think why they would then need to try to change details having already taken control of the account and emptied it?

I've also considered the possibility that A's mobile phone was successfully "cloned". It's possible to take over someone's mobile phone account and "clone" their device. But, that would likely only provide access to the number and not any other details contained on the original device. Whilst any texts sent to A's device could be accessed by a "cloned" device, it doesn't explain how the account was accessed in the first place and details changed on the Counting Up account. That's because an email sent to A's email address would also need to be responded to – which is unlikely to be available on a "cloned" device, so I don't think this is the explanation for how the disputed transactions were made.

A couldn't identify where IP address data was matching – but in the audit data provided by Counting Up for the 29/08/19 it says:

2019-08-29T10:21:04.000Z	213.205.240.135	D5824205-CC14-40BB-969A-4283641BF8BB

2019-08-29T16:24:54.000Z	213.205.240.231	59865c39-ec54-4020-9586-f9abc0647632

A's usual device ends in ….7632 and the device used to make the transactions ends with …F8BB. What this data shows is that both devices were present using the same IP address on the same day. The first three sets of numbers – here 213.205.240 relate to the location data and the last three (135/231) relate to the different devices used to connect to the internet services. So, the evidence points to the same IP address being used by both devices on the same day – something which I've already covered in my second provisional decision.

A's position is that unknown third parties breached their security and were responsible for the disputed transactions, but the evidence I've examined leads me to the objective conclusion that I think A were more likely than not responsible making these transactions or allowing someone else to do it with their authority. Whilst A have provided evidence of contact with their mobile phone & email provider from unknown third parties- the activity took place some days after the disputed transactions had already taken place. There's no evidence that explains how someone could obtain access to A's emails before the disputed transactions took place, identify the debit card details to confirm payments and be using the same IP address on the day of the disputed transactions.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask A to accept or reject my decision before 28 July 2022.

David Perry
Ombudsman