complaint

Mr V complains that Paysafe Financial Services Limited won’t refund over €11,000 made from his account, which he says he didn’t authorise.

background

In October 2015, Mr V was the victim of a scam known as ‘phishing’ (where fraudsters send an email to a customer as though it had come from a known service provider – in this case NETELLER). It’s not in dispute that what happened was an act of fraud. So I have used the term ‘fraudster’ throughout to refer to the third party involved.

Mr V held an electronic money wallet with Paysafe – his NETELLER account. On 7, 8 and 9 of October 2015 he received emails from the fraudster, posing as NETELLER, asking him to confirm his registered email address on the account. The emails asked Mr V to click on a link which was valid for seven days. It also said he needed to verify his email address as soon as possible.

Mr V says the emails looked the same as other, genuine, emails he had received from NETELLER about his account. And he recently changed his phone and so thought the emails related to him accessing his account from a new device. Mr V was worried about losing access to his account and so clicked on the link. He says he was taken to a webpage which resembled the genuine NETELLER webpage. The webpage asked Mr V to enter his password and other personal details – his email address was already pre-populated. Due to the amount of information wanted Mr V ‘gave up’ and he says he never hit the submit button.

Over the weekend of 10 and 11 October 2015 several transactions happened on the account, which Mr V says he never authorised. NETELLER had stopped one transaction but he was €11,993.50 out of pocket. The transactions are as set out below:

<table>
<thead>
<tr>
<th>Date and time</th>
<th>Status</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/10/2015 – 08.40</td>
<td>Accepted</td>
<td>3425.10</td>
</tr>
<tr>
<td>10/10/2015 – 09.09</td>
<td>Accepted</td>
<td>3425.10</td>
</tr>
<tr>
<td>10/10/2015 – 09.58</td>
<td>Declined</td>
<td>2295.60</td>
</tr>
<tr>
<td>10/10/2015 – 10.07</td>
<td>Accepted</td>
<td>2149.26</td>
</tr>
<tr>
<td>11/10/2015 – 11.17</td>
<td>Accepted</td>
<td>1134.11 reversed 19/10/2015</td>
</tr>
<tr>
<td>11/10/2015 – 11.23</td>
<td>Accepted</td>
<td>1134.11 reversed 19/10/2015</td>
</tr>
<tr>
<td>11/10/2015 – 15.44</td>
<td>Accepted</td>
<td>362.91</td>
</tr>
<tr>
<td>11/10/2015 – 16.57</td>
<td>Accepted</td>
<td>362.91</td>
</tr>
</tbody>
</table>

He discovered this early on 12 October 2015 and contacted NETELLER immediately about that. He also realised the fraudster had changed the recovery email address for the account, which meant he didn’t receive information from NETELLER about his account.

NETELLER deactivated Mr V’s account for security reasons, and it was able to retrieve €2,268.22 – shown as the reversals in the above table for 19 October 2015. It was a local NETELLER office that Mr V contacted as he wanted to speak to someone in his native language. When this was finally arranged, Mr V says he was contacted by a cleaner, not a NETELLER representative.

He was told by NETELLER on 13 October 2015 that the email sent to him had been a phishing email. Mr V was asked to complete a questionnaire about the transactions. He was also asked to provide a police report about the matter. Mr V tried to report this to local police
but was told this would need to be done in the capital. This would take some time, as it meant Mr V needed to travel there. Mr V notified NETELLER of the difficulties this would present but he says it refused to help until this was done. Mr V managed to travel there towards the end of October 2015, and he was told the police investigation was likely to take some time. Mr V notified NETELLER the matter had been reported.

I understand that police sent reports to NETELLER about the matter in February 2016 and August 2016. Mr V contacted NETELLER for an update in December 2016 and was told it would provide details of its findings should it be contacted by officials. In March 2019 Mr V complained about this matter via his lawyer. It issued a final response on 28 March 2019 declining Mr V’s request for a refund as it said is account had been compromised as a result of his intent and/or gross negligence.

Our investigator upheld the complaint. She wasn’t persuaded Mr V had acted with intent or gross negligence and so she found Paysafe ought to refund the unauthorised transactions. She also felt Paysafe had handled the matter particularly poorly and so also asked for £500 compensation for the distress and inconvenience caused.

Mr V accepted the outcome, but Paysafe didn’t. It said it didn’t agree that Paysafe should be liable to reimburse Mr V when he was the victim of phishing outside of the NETELLER wallet. Its investigation shows that whoever had access to Mr V’s account had direct access to his credentials (his e-mail, account password and secure ID). It remains of the view Mr V has been grossly negligent.

my findings

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

relevant considerations

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

The withdrawals from Mr V’s account were made in October 2015. So the relevant legislation is that set out in the Payment Services Regulations 2009 (PSRs) as Paysafe was providing payment services – electronic money issuers are payment service providers. And I’m satisfied this was a payment account. In October 2018, the Court of Justice of the European Union handed down a judgment which considered what a payment account was Bundeskammer für Arbeiter und Angestellte v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG (Case C 191/17) (4 October 2018). It’s my understanding that during its consideration, it found the defining characteristic of a payment account was the ability to both send third party transactions and receive them. As a result of this the Financial Conduct Authority changed its guidance at PERG 15.3 Q16 to include this characteristic. In its view payment accounts would include e-money accounts.
But if I’m wrong about that, the terms and conditions, which are set out below, are closely linked with PSR 2009 such that I find it fair and reasonable to take them into account.

I think these sections of PSR 2009 are of particular relevance here:

“Consent and withdrawal of consent

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

(a) the execution of the payment transaction; ...”

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

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

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

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

“Evidence on authentication and execution of payment transactions

60.—(1) Where a payment service user—

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

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

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

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

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

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

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

“Payer’s liability for unauthorised payment transaction

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

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

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

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

Intent

Intent isn’t defined within the terms and conditions of the account. I’ll therefore apply the natural meaning of intent – that being something you want or plan to do; a deliberate act.

I note the FCA’s guidance on the PSR’s 2009, which gives a helpful indication of the regulator’s view of what it means, and refers to:

- 8.108 a customer who “deliberately … failed to comply” with their obligations
- 8.116 a customer who “has intentionally … not complied with their obligations... the burden of proof lies with the payment service provider…the rejection must be supported by sufficient evidence to prove that the customer is guilty of … intentional breach”.

This guidance also gives an indication of the regulator’s view of what’s meant by taking all reasonable steps to keep [a payment instrument’s] security features safe at Regulation 57(2) PSR’s 2009:

- 8.97 says “What constitutes reasonable steps will depend on the circumstances, but payment service providers must say what steps they expect customers to take in their pre-contract disclosure information.”

gross negligence

Whether a customer has acted with “gross negligence” is something that can only be assessed on a case by case basis, taking into account all the circumstances. The term is not defined in PSR 2009 nor in the first Payment Services Directive. However, recital 72 of the second Payment Services Directive provides as follows:
“In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties…”

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

“… we interpret “gross negligence” to be a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness.”

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

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

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

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

**the terms and conditions of Mr V’s account**

Paysafe has provided a copy of the terms and conditions that apply to the account. I note these are from January 2020 as did the investigator. The investigator set out the assumption these are the same as those that applied in 2015. Paysafe hasn’t corrected that assumption and so I also proceed on the basis they are the same.

The terms that are of particular relevance in this context are:

6.5.10 You must give consent to the execution of a Transaction for it to be authorised. You agree that by pressing the ‘agree’ button, or entering your Account ID Information (or any equivalent button or process whereby you submit the required Transaction information you are confirming that you are providing consent to for Transaction to be processed and for the relevant Fees to be charged and deducted from your Account. All transactions made using
your PIN, your Account ID Information or any other security procedures that we require are deemed to be authorised by you. …

13 Keeping your account and card safe

13.1 It is your responsibility to keep your Card safe; your Card is personal to you and you must not give it to anyone else to use. You must take all reasonable precautions to keep your Account ID Information confidential and secure. This includes ensuring the ongoing security of your Account ID Information and your personal computer device for accessing the Internet. …

17 Warranties, liabilities and disclaimers

17.5 In the case of an unauthorised payment or a payment that was incorrectly executed due to an error by us, we shall, as soon as practicable, refund the payment amount including all fees deducted therefrom. This shall not apply:

17.5.1 where the unauthorised payments arises from your failure to keep your Account ID Information safe in accordance with section 13 of these Terms of Use, in which case you shall remain liable for the first £35 GBP (or equivalent in the currency of your Account) unless section 17.5.3 applies;

17.5.3 if the transaction was unauthorised but you have acted fraudulently or compromised the security of your Account with intent or gross negligence, in which case you shall be solely liable for all losses; …

The above relevant considerations means that, if the transactions Mr V says were unauthorised, it would be fair and reasonable for Paysafe to refund the full amount taken, unless, with intent or gross negligence, Mr V failed to comply with the account terms and conditions (and the obligations set out in Regulation 57).

There are two key questions relevant to my consideration of what is fair and reasonable in the circumstances of this complaint:

1. were the disputed transactions authorised by Mr V? and;
2. if they weren’t, did Mr V fail with intent or gross negligence to comply with his obligations under the PSRS’s 2009 – in particular, did he fail to comply with the terms and conditions of his account, or to keep his personal security features safe?

Were the disputed transactions authorised by Mr V?

Regulation 55 says that the payer must give consent, and it “must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider”. The payment services directive itself (which PSR 2009 implements) says “In the absence of such consent, a payment transaction shall be considered to be unauthorised.”

The disputed transactions were made on-line. There is nothing within the account terms and conditions which sets out the exact form and procedure required for payments to be made on-line. However. 6.5.10 says:

You must give consent to the execution of a Transaction for it to be authorised. You agree that by pressing the ‘agree’ button, or entering your Account ID Information (or any
equivalent button or process whereby you submit the required Transaction information you are confirming that you are providing consent for the Transaction to be processed and for the relevant Fees to be charged and deducted from your Account. All transactions made using your PIN, your Account ID Information or any other security procedures that we require are deemed to be authorised by you. …

Our investigator queried what steps are necessary for a transaction to be completed. Paysafe confirmed the customer would need to log onto the account using the customer's email and password and that a Secure Identification number is required to complete a transaction. So it seems to me that in order to complete a transaction Mr V would need to:

1. log on to his account using his email and password;
2. provide information about who he wanted to pay;
3. provide his Secure ID to complete the transaction.

Mr V says he clicked on a link which took him through to a webpage which looked like NETELLER's website. He provided information, which he believed, was to authenticate his email address. This seemingly included logging onto his account. Mr V says he didn't submit his details. I think he likely did. But it is possible the email contained keylogging software which meant that even if Mr V didn't hit submit, the fraudsters will have gained the information needed to be able to log into his account, using his credentials.

Given that it wasn't actually NETELLER's website that he was logging onto, it’s questionable whether Mr V completed even the first step to authenticate a payment. Nevertheless, I'm satisfied Mr V didn't complete the remaining steps as he didn't know payments were made from his account until he checked it on the morning of 12 October 2015. He also didn't recognise the payee although it was clear this was another NETELLER account holder as the payments were recorded as member-to-member payments.

On balance, I'm not persuaded Mr V completed the steps required for the payments to be considered authorised. So it follows they were unauthorised.

**Did Mr V fail with intent, or gross negligence with the terms and conditions of the account, or to keep his personalised security details safe?**

I need to consider whether Mr V appreciated that his actions, or inactions, in the circumstances meant he wasn’t complying with the terms and conditions of his account; or that he appreciated he wasn’t taking all reasonable steps to keep account information and security details safe. In the circumstances, I don’t think Mr V failed to comply with his obligations with intent.

Mr V says he received several emails that appeared to be genuine NETELLER emails. He said he had received emails before, and they looked the same. He wasn't surprised to receive the emails as he had just changed his phone and so was accessing his account from a new device.

I have seen a copy of the email Mr V was sent. I agree with Mr V, this does look like a genuine email. And it does explain that Mr V needs to verify his email as soon as possible. Mr V says he clicked on the link as he didn’t want to lose access to his funds. And when he did so he was taken to a webpage that looked the same as NETELLER's genuine website. I haven’t seen a copy of that, but I have no reason to doubt what he’s said, given the email I have seen.
NETELLER has confirmed the email wasn’t genuine. I have no reason to doubt the webpage wasn’t either. I’m not persuaded Mr V knew or appreciated this when he clicked on the link, or when he entered his account and security details. Although Mr V says he didn’t hit the submit button either he did, or the fraudsters didn’t need him to as the email could have contained keylogging software – a known method used by fraudsters. I don’t think Mr V would have realised that by entering his details, whether he hit submit or not, would allow his details to be obtained by a fraudster.

I accept that by completing the log in process and inputting his personalised security features, Mr V did give this information to a fraudster. But I can’t ignore that he did this in order to retain access to his account and he thought he was doing so on a genuine webpage. I don’t think he realised or appreciated he’d been tricked or that he wasn’t complying with his account terms and conditions or was failing to take reasonable steps to keep his account and personalised security information safe. It follows that I don’t find Mr V failed to comply with his obligations under the account terms and conditions with intent, as he didn’t appreciate the true nature of what he was doing.

I turn now to whether Mr V acted with gross negligence. I have considered whether the actions Mr V took fell so far below the standard of a reasonable person that he failed with gross negligence to take reasonable steps to keep his account information and personalised security information safe or to comply with the terms and conditions of the account.

As set out earlier, negligence is often referred to as a failure to exercise reasonable care. And the use of ‘gross negligence’ rather than ‘negligence’ suggests a lack of care that goes significantly beyond ordinary negligence. So I’ve thought about Mr V’s actions and what a reasonable person would do in his circumstances.

It’s important to take into account all the circumstances when considering whether an individual’s actions amount to gross negligence. Scams such as the one experienced by Mr V are sophisticated.

Paysafe has argued that it shouldn’t be held liable for the disputed transactions as Mr V was the victim of phishing outside of the NETELLER wallet. It also says whoever had access to Mr V’s account had direct access to his credentials.

I have thought carefully about this. But I’m not persuaded that the phishing happening outside of the NETELLER wallet bears any relevance to whether Mr V was acting with gross negligence. Phishing is a well know scam used by fraudsters to trick account holders into believing they have received emails from a genuine account provider, with links to fake websites. By its very nature phishing will always occur outside of a genuine provider’s systems – that is the very point of the scam.

It’s not in dispute that Mr V shared his account details and security information. But that of itself isn’t enough for me to find he acted with gross negligence; I also need to consider the circumstances in which those details were shared. I need to bear in mind that Mr V believed he had received a genuine email from NETELLER about verifying his email address. Against a backdrop of his changing his phone recently, I don’t think him receiving this email ought to have alerted him to anything untoward happening; he was using a new device and so thought email verification was a legitimate request from NETELLER.
As mentioned above, having seen a copy of the email, I can understand why Mr V thought it was genuine. I don’t think it was until Mr V noticed funds had gone from his account, or NETELLER confirmed it, that he realised the email might not have been genuine.

As mentioned above, I haven’t seen the webpage that Mr V was presented with when he clicked on the link in the email. As he was accessing the link via what he thought was a genuine email, I have no reason to doubt Mr V thought he was on the real website. Indeed, Mr V has said as much; that the website resembled NETELLER’s webpage/online environment. The webpage requested he complete his personal details and provide his password. And he says the email address had already been completed for him.

As Mr V believed he was on NETELLER’s genuine website, there would have been no reason for him to question the information he was being asked for. It was in the context of verifying his email address that the information was given. I think a lot of people in a similar situation would have behaved in the same way as Mr V. It follows that I don’t think the actions Mrs V took fell so far below the standard of a reasonable person, such that I would find he failed with gross negligence to keep his account information and security details safe or comply with the terms and conditions of his account.

**Other matters**

Mr V made NETELLER aware of the fraud on the morning of 12 October 2015. This was just one day after the last disputed transaction. Although it sent Mr V a questionnaire and requested a police report, I cannot see any evidence that it actually investigated the fraud at the time.

I know it managed to recover a total of €2,268.22. But despite a police report being sent to NETELLER in February and August 2016, it didn’t do anything further about the fraud until Mr V complained, via his lawyer, in 2019.

Whilst I accept notifying the police of the fraud was part of its requirements at the time, I see no reason why a police report was required before NETELLER could start or even complete its investigations. It is, after all, the party that is required to show that disputed transactions are authorised or, if not, the account holder has acted with gross negligence or intent to not comply with the account terms and conditions. Failing that, the money should be refunded.

NETELLER took none of those steps until Mr V raised a complaint in 2019. I consider this to be very poor customer service and means that Mr V has been out of pocket for far longer than he ought to have been. I therefore agree he should be fairly compensated for that.

**putting things right**

I am upholding this complaint and require Paysafe to:

- Refund the unauthorised transactions of €9,725.28 (the disputed amount less those already reversed) less the £35 allowed for in the account terms and conditions (if it chooses to retain this).
- Pay Mr V £500 – or the Euro equivalent - for the inconvenience he has been put to as a result of Paysafe not settling this matter much sooner.
**my final decision**

For the reason given, I uphold this complaint and require Paysafe Financial Services Limited to redress Mr V as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr V to accept or reject my decision before 2 August 2020.

Claire Hopkins  
ombudsman