DRN-5356429

The complaint

A company which I'll refer to as 'B' complains that Stripe Payments UK Limited won't refund the money it lost as the result of a scam.

The complaint is brought on B's behalf by its director, Mr B.

What happened

Both parties are aware of the circumstances of the complaint, so I won't repeat them all here. But briefly, B had outstanding invoices received in January 2024 from one of its suppliers, who I'll refer to as 'T'. In February 2024, B received an email from T's director asking when these outstanding invoices would be paid. B's accounts team confirmed that the payment would be made at the end of February 2024 in line with B's usual process.

Shortly after the email was sent from the accounts team, B received a further email from T's director which said T's account was being audited and therefore the invoices would need to be paid to a subsidiary account. B says there was nothing on the email that led the accounts team to be suspicious and as the invoices were expected, it added the new account details and made a payment for £39,185.97 on 29 February 2024. Although unknown at the time, a scammer had intercepted the email exchange between B and T and amended the payment details. The payment went to an account held with Stripe.

The day after B had made the payments to the new account details, the genuine supplier contacted B to ask why its invoices hadn't been paid and the scam was uncovered. B immediately contacted its bank, and it says it was told there was a good chance of recovering its funds as it had raised concerns quickly. B's bank raised a fraud request with Stripe, but unfortunately B's funds couldn't be recovered. B was unhappy that Stripe had allowed a scammer to open an account and not detected that its funds had been received as a result of a scam, so it made a complaint.

Stripe said that it would review the conduct of its customer and see whether they had breached its service agreement and take action if necessary. B was unhappy with Stripe's response and asked our service to look into its complaint. Shortly after, Stripe responded to say that it didn't believe B was able to make a complaint against it as Stripe was only the recipient of the funds received by the scammer, and shouldn't be treated as the respondent business.

Our investigator recommended the complaint be upheld. She said that under the Dispute Resolution (DISP) rules, she was satisfied that B had the relevant relationship with Stripe so that we could consider B's complaint. The investigator said that due to the limited information provided by Stripe, she wasn't satisfied that it had undertaken sufficient checks before opening the account for its customer. She also said that Stripe told our service it had undertaken a risk review once its customer had received funds from B, but there were insufficient risk signals to warrant a further review. However, Stripe hadn't evidenced the checks it had undertaken or that these were proportionate. So, the investigator thought that Stripe should refund B's loss of £39,185.97 along with 8% interest for the time that B had been without its funds, and £300 compensation for the inconvenience caused.

Stripe didn't agree with the investigators opinion and asked for an ombudsman to review the complaint. It provided further evidence of its account opening checks and the risk review that took place when B's payment was received.

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 done so, I've decided to uphold it for broadly the same reasons as our investigator. Stripe has an ongoing obligation to be alert to various risks in relation to accounts with it, and it is expected that Stripe conducts its business with due skill, care and diligence. There is also an expectation that Stripe has systems in place to look out for unusual transactions or other signs that might indicate that its accounts are at risk of fraud.

It is a commercial decision that Stripe is able to make on how it chooses to meet its legal and regulatory obligations to prevent its accounts being used for fraudulent purposes. It is also Stripe's decision on how it chooses to strike the balance between allowing its customers to transact business and questioning transactions to confirm they are legitimate. But my role is to look into the circumstances of the case and based on what I have seen, decide whether I think Stripe could and should fairly and reasonably done more.

Stripe has provided information to our service to allow us to investigate B's complaint. I am limited as to how much information I can share because it relates to a third-party account. But I'd like to assure B that I've carefully reviewed everything before reaching my decision.

From the evidence provided, it appears the Stripe's customer opened the account roughly two weeks before the payment from B was received into the account on 29 February 2024. Stripe says that it hasn't done anything wrong as it followed its process and undertook sufficient checks for its customer before it opened the account. It also says that it verified its customers name and address. Our service has requested evidence from Stripe to show the documents it obtained to open the account on several occasions. But the only evidence supplied by Stripe was to say that it obtained a copy of the customer's passport. There was no evidence that it obtained proof of individual or business address.

Additionally, the account opening information Stripe has provided shows the merchant categorisation code industry type provided by its customer. However, a simple Companies House search shows that the type of business registered for its customer didn't match, and I haven't seen any evidence that this was queried by Stripe. Based on the evidence provided, I'm not persuaded that Stripe undertook sufficient checks before opening this account for its customer.

I acknowledge that had Stripe asked its customer for further information, they may have been able to provide this. I also recognise that had Stripe declined to open the account, that its customer may have opened an account elsewhere and the scam would still have taken place. However, in this case I think Stripe should have done more to prevent the scam and loss of B's funds. I say this because Stripe told us that it undertook a risk review of its customer's account on the day B's funds were received, but it had no concerns. Stripe hasn't told us what checks it undertook; however, it has told us that the account should only be used by customers to add funds to the balance of their own account, not for peer-to-peer transactions or customers. In this case, I can see that the first payment into the account held with Stripe was from B, not its own customer.

I'm satisfied that this transaction was in breach of Stripes own account terms and conditions, so I think it ought reasonably to have flagged that something wasn't quite right. Had Stripe undertaken sufficient checks, I think it would have identified that not only had a payment been received from a totally different company name, the payee name also didn't match the name of its customer. I think these inconsistencies, along with the new account opening, ought to have indicated to Stripe that is customer may not have been the intended recipient of B's payment. So, I think it would have been reasonable for Stripe to ringfence these funds until it had received further information, such as proof of entitlement of these funds from its customer. On the balance of probability, I don't think Stripe would have received anything meaningful from its customer by the time it was contacted by B's bank on 1 March 2024.

Stripe told us that I was only notified of the scam in August 2024, by which point the funds had already left the account. However, I've seen evidence from the sending bank which shows that it contacted Stripe about the scam on 1 March 2024, the day after the funds arrived. Stripe told us that its customer didn't actually debit payments from the account until 5 March 2024 and 7 March 2024, therefore I think that Stripe missed an opportunity here to prevent the financial loss caused to B. And, as a result I think it also caused avoidable inconvenience.

For completeness, I've also considered whether B should bear some responsibility for its loss due to any contributory negligence. As I understand it, it was the supplier's email which was hacked and as such the email address from which B received the emails wasn't suspicious. B was expecting the invoice it received, and as the scammer used personal names and similar tone there was nothing to alert it that there was an issue. But even if I did think there was some failure on part of B, it does not negate the fact that Stripe missed the opportunity to prevent B's loss, as described above.

Putting things right

I'm satisfied that Stripe had the opportunity to prevent B's loss when it was contacted by B's bank before the funds had left its customer account. And I think its actions caused B inconvenience.

To put things right I think Stripe should refund B's loss of £39,185.97. Stripe should also add annual interest at 8% simple from the 1 March 2024 when it was notified of the scam to the date the funds are returned, to reflect the time that B has been deprived of the use of those funds. I also think it should pay £300 for the inconvenience caused.

My final decision

My final decision is that I uphold this complaint. I direct Stripe Payments UK Limited to resolve the complaint in the way I have set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask B to accept or reject my decision before 16 July 2025.

Jenny Lomax
Ombudsman