DRN-4068477

The complaint

A limited company, which I'll refer to as T, complains that WorldPay Limited unfairly charged it fees following a card testing attack. T says that WorldPay's negligence facilitated the attack and WorldPay also failed to assist it in stopping the attack.

What happened

On 7 September 2022, T contacted WorldPay to inform them that T was being targeted in a card testing attack. T made several calls to WorldPay over the next few days, asking for help in stopping the attack.

Ultimately, over the course of around a week, over 12,000 card payment transactions were attempted, through a non-customer facing installation that T used for internal processing of telephone orders. Most of the transactions were for £1 and most were declined. T attempted to refund all the successful transactions.

WorldPay's subsequent invoices included fees as a result of the card testing transactions, largely a per transaction authorisation fee, but also fees to process refunds and fees for chargebacks on the refunds T missed.

T complained to WorldPay, but WorldPay didn't uphold the complaint. They said that a vulnerability in T's own website had enabled the card testing to occur and that it was therefore not the responsibility of WorldPay.

WorldPay later also said that in 2017, T had also requested the removal of CAPTCHA from the telephone order installation that was attached. T had signed an agreement acknowledging the increased risk that removing CAPTCHA exposed it to at that time.

T disagreed and referred its complaint to the Financial Ombudsman Service. It said:

- The vulnerability was in WorldPay's gateway not T's website.
- Its investigations showed that there was a flaw in WorldPay's systems, which made it easy for fraudsters to identify valid installation IDs and then use WorldPay's own publicly available code to carry out card testing.
- WorldPay's installation IDs were also only seven digits long, so could be found by "brute force" attack. T had no control over this, it was entirely WorldPay's responsibility. There had been no change to WorldPay's payment page since at least 2009.
- T considers that this means that WorldPay are effectively assisting the fraudsters by not improving their security. WorldPay had refused to engage with T about this.
- It had had exactly the same problem with card testing in 2017. WorldPay had been difficult on that occasion too, but had eventually agreed to refund all their fees.

- Did WorldPay not have a duty of care to its customers and to those individuals whose cards are being tested?

- WorldPay was now saying that the use of CAPTCHA is crucial. If that was the case, WorldPay should make it compulsory - or at least have suggested reinstatement earlier or sent yearly reminders.

- T had made 17 calls to WorldPay during the attacks with a total duration of six hours and 43 minutes. But WorldPay never mentioned CAPTCHA in those phone calls.

- If WorldPay had mentioned reinstalling CAPTCHA, which it presumed could be done instantly, then that could have stopped the attack.

In the course of our investigation, WorldPay said:

- WorldPay sets CAPTCHA as enabled by default as a security measure, as this was an industry standard.

- By signing the agreement authorising the removal of CAPTCHA from their telephone order installation, T had understood and accepted that it was exposed to increased risk.

- It was impossible completely to prevent card testing, but the use of CAPTCHA deterred it strongly, as it made it difficult to automate. They had written to T about this in 2017 when T was last attacked by card testers.

- The interface T was using ("Select Junior used as Virtual Terminal") was specifically for merchants wanting to key in sales taken over the phone. It was a hosted payment page, designed to be integrated into a third party or bespoke virtual terminal, which the merchant used to input sales. In 2017, they had pointed out that Select Junior was a relatively simple interface and there were others available that might offer more security.

- They appreciated the effort T had gone to to explain how the card testing could have been carried out, but this was entirely speculative.

- WorldPay took fraud seriously, but fraud prevention was a byproduct of their business rather than being primary. They didn't provided any fraud monitoring services to T, nor were they obliged to do so under the terms of the contract.

WorldPay initially said they couldn't find any of T's phone calls. When they found them, our investigator concluded that the card testing could have been halted earlier if WorldPay had offered to turn off the relevant installation ID straight away rather than just email a department with a five day turnaround time. Our investigator also pointed out some errors in WorldPay's customer service.

WorldPay replied accepting that they "could have taken the unorthodox action to disable the merchant's installation during a call on 7 September", even though the standard process was to email the request with a five working day timescale. They also acknowledged some poor customer service. In the light of this, they offered to refund 50% of the fees amounting to £815.42.

T didn't accept this offer as it felt WorldPay should refund 100% of the fees. So the file was passed to me to reach a final decision.

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.

I think both sides agree that it's likely T has been the victim of a fraudulent practice known as high volume card testing. This is where fraudsters attempt a large number of low value online payments with a merchant to check if stolen card details are still valid or to search for valid card numbers. Automated bots or scripts are often used to carry out a large amount of card testing transactions in a very short period of time.

Is WorldPay entitled to charge authorisation fees for card testing transaction?

I think it's worth me setting out at this point that I'm not aware of any regulations that require merchant acquirers to do anything to protect their customers from card testing specifically. I'm also not aware of any regulations that prevent the acquirer from charging for transactions resulting from card testing. My starting point is therefore to look at the terms of the contract between WorldPay and T.

The contract comprises several documents, including the Merchant Services Agreement ("MSA"), Application Form and the Customer Operating Instructions. These documents collectively set out the responsibilities and liabilities of the parties. The first thing I have considered is whether WorldPay has complied with the terms of this agreement.

T's application form shows that a per transaction authorisation fee was included from the very start. I don't think T disputes that it was aware of this fee and that it was part of its contract. The previous card testing attack it experienced in 2017 would also have made it aware that this fee was payable on card testing transactions, albeit that on that occasion, as this time, T argued that it was unfair to charge it in these particular circumstances.

The MSA says that the merchant (in this case T) is "solely responsible for establishing and applying adequate security systems and procedures." And the merchant is "responsible for all losses resulting from any unauthorised activity." I think this makes it clear that WorldPay don't accept responsibility for attacks on the security of T's payment arrangements.

Having examined the documentation, I've reached the same conclusion as our investigator, namely that the contract permits WorldPay to charge a fee for each authorisation attempt. There is no exception for card-testing.

How did the card testing occur and has WorldPay made an error in this case?

This is an unusual case in that the installation that the fraudsters used wasn't customer-facing. It was a virtual terminal installation used for T's staff to key in telephone orders. It therefore couldn't by its nature have as high a level of security as a customer-facing website, for example, 3D Secure, but it also wouldn't be expected to be exposed to as much risk.

T's representatives believe strongly that vulnerabilities in WorldPay's payment systems were exploited to carry out the card testing, particularly WorldPay's seven digit installation IDs. T has shown in some detail a method by which it could have been carried out, using publicly available information and code. I agree that this is a possibility, but it is also, as WorldPay pointed out, speculative.

I haven't seen any evidence of how the attack was actually effected and my understanding is that this isn't clear. I don't think I can fairly say that it's more likely than not that WorldPay's potential vulnerabilities were exploited rather than T's, particularly as the contract makes it clear that T is responsible for establishing security systems.

I appreciate that T considers that WorldPay has been negligent in failing to improve the security of its gateway, for example, by making its installation IDs harder to extract or deduce. But we don't know what enabled the fraudsters to find their way in here. And I can see that from WorldPay's perspective, this isn't a straightforward issue. WorldPay is primarily a payment facilitator and changing its IDs would cause considerable disruption for many customers.

I think it's also fair to say that T has chosen to contract with WorldPay in the knowledge of what it believes to be shortcomings. T continued to use WorldPay as its merchant acquirer having been impacted by card testing in 2017. WorldPay refunded the charges on that occasion, but only after making it clear that this was a goodwill gesture not an admission of any liability. I realise that changing providers once software is embedded may not be straightforward, but this is a liquid market, with many other providers of merchant services available.

I've also seen the email WorldPay's Chief Information Security Officer wrote to T after the 2017 card testing attack. In this, he said:

> "We have taken a series of actions on a number of fronts to improve security and stop this activity, the most visible of which is CAPTCHA, but our security response is by no means limited to this.
>
> The CAPTCHA implementation that we now offer on the payment page in question has been shown to be the quickest, most effective solution with no technical burden on existing Worldpay customers, and the least impact on conversion. It is now in use by many tens of thousands of customers and is proving to be effective at stopping these type of incidents.
>
> However, we understand that this may not be the desired shopper experience in your case, and therefore, we would recommend an alternative integration type to Select Junior.
>
> The Select Junior integration method offers a very simple API which is easy to use with low customer development effort. In particular, it is designed so that it does not require any kind of dynamic scripting on your server.
>
> If you wish to have an increased level of mutual authentication, we would also encourage migration to our XML or JSON APIs, which are specifically designed to meet the needs of larger enterprises".

T chose to remove CAPTCHA from its telephone order installation, having signed to accept that this exposed it to higher risk. T has also told us that it did not make any changes to its set-up after the 2017 attack and the receipt of the email containing the above.

I know that T thinks that WorldPay owed it a higher duty of care and should have reminded it annually about CAPTCHA since 2017. But WorldPay never said they would do this and there was nothing in the contract obliging them to, so I don't think it would be fair to put the onus on WorldPay, especially as they highlighted the risks clearly when T first requested the removal of CAPTCHA.

For all these reasons, I don't think I can fairly say that the card testing was caused by any negligence or error on the part of WorldPay.

Next I listened to the phone calls T made during the attack, WorldPay have accepted that their customer service was poor and I agree with this assessment. In many hours of calls, WorldPay frequently misunderstood things, required endless repetition of the circumstances and made several suggestions that were inaccurate or irrelevant. I agree with T that I haven't heard CAPTCHA mentioned at any point and that this would have been helpful.

WorldPay have also agreed they could have done more to help earlier, albeit that they characterise the solution of turning off the relevant installation ID temporarily as "unorthodox". One of WorldPay's operatives proposed this solution on 8 September, but by then, a large proportion of the transactions had already taken place over the night of the 7/8 September.

Next I've considered what constitutes fair compensation for these failings – that is, whether WorldPay's offer is fair.

Putting things right

WorldPay have offered to refund half of the fees incurred from the card testing, amounting to £815.42. Our investigator thought this was fair, but I know that T's representatives feel they should get a full refund.

I'm conscious that, although WorldPay has made mistakes, they didn't cause the card testing and I haven't been persuaded that it was more likely than not vulnerabilities at their end that facilitated it. I'm also aware that they too incur charges as a result of the card testing transactions.

I'm also mindful that T has had past experience of card testing, which it believes was effected in the same way, and chose not to take any steps to mitigate the risk.

I realise that being the subject of a card testing attack is a distressing, costly and time-consuming experience, which was made worse by WorldPay's poor customer service. However, on balance, I consider this to be a fair offer by WorldPay in all the circumstances, so I'm not going to ask them to do anything more.

My final decision

I uphold this complaint. WorldPay Limited has already made an offer to settle the complaint and I think this offer is fair in all the circumstances. So my decision is that WorldPay Limited should pay T £815.42.

Under the rules of the Financial Ombudsman Service, I'm required to ask T to accept or reject my decision before 12 July 2023.
Louise Bardell
Ombudsman