DRN-4337593

The complaint

Mr M is unhappy that PayrNet Limited loaded an adverse fraud marker against his name.

What happened

As both parties are familiar with the circumstances of this complaint, I've summarised them briefly below.

Mr M held an account with Rewire, an agent of PayrNet. In August 2022, PayrNet received notification from a third-party bank that Mr M's account was the confirmed beneficiary of fraudulent funds.

PayrNet looked into the report and could see the funds enter Mr M's account and were then immediately withdrawn to a cryptocurrency platform. As a result, Mr M's account was closed, and it loaded an adverse fraud marker against Mr M's name on the Cifas database.

Mr M discovered the marker had been placed after his banking facilities with another provider were withdrawn. He made a complaint to PayrNet but says he didn't receive a response. So, he referred his complaint to our service.

Mr M told our service that at the time the account was closed, he'd lost his mobile telephone device in the gym. He reported it to staff at the gym, tracked the device on an application and sent a message to it asking the finder to return it.

Several weeks later, Mr M says his device was returned to staff at the gym and he thinks that a third-party had used it to access his account while it was not in his possession.

An Investigator considered the evidence provided by both parties and concluded PayrNet hadn't loaded the marker fairly and in line with Cifas guidance. They recommended PayrNet remove the marker and pay £150 in compensation for the distress and inconvenience caused.

PayrNet disagreed. It argued that there were several inconsistencies in Mr M's testimony, provided evidence of bad character and it defended its position on the marker being loaded fairly.

As PayrNet disagreed with the Investigator's opinion and recommendations, the matter was passed to me for a decision.

On 25 August 2023 I issued provisional findings to both parties setting out what I was minded to conclude on the complaint. The provisional decision was as follows:

'*One of the relevant considerations here are set out by Cifas: the fraud marker database controller. In its Handbook—which members must adhere to when loading markers—it sets out the burden of proof the member must meet. The relevant standards applicable to this complaint are:*

- *That there are reasonable grounds to believe that a fraud or financial crime has been committed or attempted.*
- *That the evidence must be clear, relevant and rigorous.*

These standards mean that PayrNet must have more than mere suspicion when loading a marker against a person's name. It must have strong evidence to support that a financial crime has been committed or attempted and that the person to whom they are loading the marker against is more than likely to have had witting involvement.

I'm satisfied that the first of the above two pillars have been evidenced here. While it has taken PayrNet an unacceptable amount of time to provide our service with evidence relating to this case, it has eventually provided us with a report from a third-party bank supporting the fact that Mr M's account received funds from a confirmed fraud. Therefore, I'm satisfied that PayrNet has demonstrated that there are reasonable grounds for it to believe a fraud has been committed.

Moving onto the second of the above two standards. PayrNet is a member of Cifas and should be aware of the rules that Cifas has set out when loading information to its database.

In June 2020, Cifas set out guidance for its members when dealing with potential 'money mules'—a term used for account holders that launder the proceeds of crime through their account(s). Within this guidance, Cifas placed certain requirements on its members that should be undertaken before a loading is added. Among other things, the main requirement is that a member contacts its customer—by more than one method—to give them an opportunity to explain the activity. This is to ensure vulnerable customers, or those that have been a victim of fraud themselves, aren't unfairly loaded to the database.

In the circumstances of this complaint, I have been provided with no evidence to show that PayrNet made any attempt to contact Mr M and give him an opportunity to explain the activity. Instead, Mr M's account was closed and the Cifas marker loaded.

While PayrNet has clearly breached these requirements here, I must consider the information I do have available, which includes Mr M's own testimony.

Mr M has told our service that he believes a third-party took control of his account after he'd lost his device in a gym. He says that it's likely that the person who took his device managed to guess his PIN that allowed access to it, as it was easy to guess.

I've considered Mr M's testimony carefully but am minded to agree with the points made by PayrNet regarding its plausibility.

Mr M's claim that he'd lost his device isn't supported by any evidence. He didn't report the theft to the police, despite it being lost for several weeks, and there is no way our service can verify his claims that he'd reported it to members of staff at the gym. Mr M doesn't appear to have made any attempt to ask staff to investigate the theft or have CCTV cameras reviewed at the venue.

Mr M has also claimed that he was tracking the device for the weeks it was missing yet he did nothing with this information. He didn't ask police to attend the location where the device was shown. Nor did he attempt to get it back himself.

Furthermore, I find Mr M's suggestion that the third-party managed to guess his PIN, as it was simply his date of birth, to be unpersuasive. Had Mr M left his device on one of the machines within the gym, it's likely it would have been taken by an opportunistic thief rather than a person known to him. Mr M has also made no claim or suggestion that anything other

than his device was stolen, such as a wallet containing identity documents. Therefore, it's unlikely that an opportunistic thief would have known his date of birth, or indeed that it was even Mr M's device. I therefore find it unlikely they would have been able to guess his date of birth and subsequently his PIN.

As well as the above, I find it unlikely a third-party who stole Mr M's device and used it to carry out fraudulent activity would have then gone to the effort of returning it to the gym considering the value of most modern-day smart devices.

My intention here is not to accuse Mr M of dishonesty or implicate him in the fraudulent activity that took place; that is not my role. I'm merely making an assessment on whether PayrNet has sufficient evidence to support the loading in line with guidance set out by Cifas. And when considering the above points I've made, I find it does. As such, I won't be asking it to remove the marker applied against Mr M.'

Both parties were provided until 8 September 2023 to provide any further comment or evidence before reaching my final decision.

PayrNet responded stating it had nothing further to add. But Mr M responded stating he disagreed with the provisional findings and provided further comment. In summary, he argued:

- He didn't pursue the phone because he has strict parents.
- His name was shown on the wallpaper of his device. He believes a search online would have revealed his date of birth.
- The geographical location of the gym where the phone was lost would have revealed the area in which he lived, again giving the thief an opportunity to find him online.
- Some of the people that attend the gym follow him on social media channels.
- Access to the banking app for his account isn't protected and can be signed into automatically.

Now that both parties have responded to my provisional findings, I'm in a position to reach my 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 have carefully considered Mr M's further submissions, but this hasn't persuaded me to change the outcome I've indicated in my provisional findings.

Mr M has said that he didn't contact the police, nor pursue the location of his device, as he has strict parents. However, I fail to understand why this would have prevented Mr M from taking action.

I'm not persuaded that any action Mr M would have taken to recover his phone would have required the involvement of his parents. I also fail to see how Mr M would have been able hide the fact that he'd lost his phone from his parents as he wouldn't have been contactable until either his phone was returned several weeks later, or a new SIM card had arrived.

Mr M has also provided several ways in which the opportunistic thief may have managed to get into his phone using his PIN.

Firstly, I'm not persuaded that Mr M's name being on the wallpaper of his device would have

been sufficient for a thief to obtain his PIN. The suggestions that Mr M has made are on the presumption that the thief knew or suspected that the PIN to his device was his date of birth. I fail to see how a third-party unknown to Mr M would have known this.

Secondly, from a cursory search online, I've seen a number of people on social media platforms bearing the same name as Mr M. I see no way in which a person who merely had access to Mr M's locked phone would know which to investigate.

I've also checked the third-party website and social media platform Mr M has suggested the thief likely would have been able to obtain his date of birth from, but both only show a partial date of birth.

For the above reasons, I find it unlikely that a thief would have been able to access Mr M's phone by guessing his PIN was his date of birth. And even if I were to accept that a third-party knew Mr M's PIN would be his date of birth, I'm not persuaded that they would have been able to find it online.

I also remain unpersuaded that an individual that stole Mr M's phone and then used it for fraudulent activity would then return the device to the location they stole it from rather than sell it for financial gain.

Mr M has further argued that the banking application that accessed his account wasn't security protected and I've failed to include this information in my provisional findings. I was aware of this when writing my provisional decision. However, I cannot see any relevance in referring to this where I see no reasonable explanation as to how a third-party would have accessed Mr M's device to open the banking application.

My final decision

For the reasons I've given above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 9 October 2023.

Stephen Westlake
Ombudsman