IN THE STATE COURTS OF THE REPUBLIC OF SINGAPORE

[2026] SGSCT 11

Small Claims Tribunals – Claim No 20703 of 2025

Between

JGX

… *Claimant*

And

JGZ

… *Respondent*

GROUNDS OF DECISION

[Banking — Credit cards — Unauthorised transactions — Phishing scam — Apportionment of loss—Whether the customer acted with gross negligence]

JGX
v
JGZ

[2026] SGSCT 11

Small Claims Tribunals – Claim No 20703 of 2025
Tribunal Magistrate Joel Tan
9 March 2026, 12 June 2026

12 June 2026

Tribunal Magistrate Joel Tan:

Introduction

1 The proliferation of digital payment systems has brought unprecedented convenience, enabling seamless transactions through mobile devices and contactless payments. However, this technological advancement has simultaneously created new vulnerabilities that sophisticated fraudsters have learned to exploit.

2 One such fraudulent scheme, as I understand it, begins with scammers deceiving victims into divulging their credit card credentials. These phishing operations lure unsuspecting cardholders into entering their primary account numbers, expiry dates, and security codes. Armed with this stolen information, the scammer then provisions the victim's card details into a digital wallet application on their own mobile device.

3 When the scammer enters the victim's card details into their digital wallet, the system initiates a process known as tokenisation. This security mechanism replaces the victim's actual card details with a unique device account number that serves as a cryptographic substitute for the original credentials. The tokenisation process typically requires authentication by the cardholder. A common means of authentication relied upon requires entering a one-time password sent by SMS to the cardholder. However, scammers often obtain these passwords through phishing, and I understand that security and authentication measures in respect of the tokenisation process have been augmented or are in the process of being augmented to combat such scams in recent years.

4 Once tokenisation is complete, the scammer possesses what effectively amounts to a digital key to the victim's credit card. The scammer can now conduct fraudulent purchases and payments using their device. The issuing bank will then seek payment from the victim for the charges relating to the fraudulent transaction. Should the cardholder dispute the transactions as unauthorised, the credit card scheme typically provides a chargeback mechanism that may reverse the settlement process, and possibly result in merchants bearing the risk of loss. However, merchants can shift this liability by demonstrating that the transactions were secured according to industry standards. Where merchants successfully establish such authentication, the loss typically falls either upon the issuing bank or upon the victim, depending upon the contractual apportionment of loss and the specific circumstances.

5 The present case concerns the question of how risk should be allocated between the victim—the claimant—and the issuing bank—the respondent—in circumstances where fraudulent tokenised transactions have occurred.

Facts

The unauthorised transactions

6 On 4 June 2024 at or around 11.14pm, the claimant's credit card, issued by the respondent bank, was successfully added to the digital wallet of an Apple device without his initiation. Despite receiving notification alerts by SMS that evening and further alerts on 6 June and 12 June respectively, the claimant took no remedial action in response to these warnings.

7 Between 17 June and 23 June 2024, a series of 22 transactions were charged to the claimant's credit card account. The claimant had not made these transactions. The transactions, executed through Apple Pay, were denominated in Japanese Yen and processed by merchants operating within Japan's stored-value electronic money ecosystem including Suica, PASMO, ICOCA, and ANA Pay. These transactions served to load monetary value into these prepaid wallet systems. Once loaded, such balances may, among other things, be spent at participating merchants.

8 The aggregate amount of these transactions totalled JPY 430,000. Applying the exchange rates utilised by the respondent bank at the time of processing, this sum corresponds to S$3,811.72 in charges added to the claimant's credit card balance, for which he was liable to the respondent bank.

9 The claimant did not receive notifications from the respondent regarding these transactions because his credit card account was configured to send transaction alerts only for purchases of S$500 and above—the default threshold setting. Since each of the 22 transactions fell below S$200 equivalent, none triggered the notification system.

Discovery of the unauthorised transactions and attempted chargeback

10 On 23 June, the respondent flagged these transactions as suspicious after noticing the pattern and attempted to contact the claimant via telephone to verify whether he had made the transactions. This attempt proved unsuccessful. The respondent therefore took the pre-emptive safety measure of blocking the credit card temporarily to prevent further transactions. The respondent sent a further SMS that day to inform the claimant of the blocking of the credit card for security reasons. This resulted in the claimant calling the respondent to confirm that he did not authorise the transactions, whereupon the card was blocked permanently and the tokenisation undone.

11 The claimant was advised by the respondent to complete the bank's dispute declaration form. The claimant submitted this on 22 July 2024. His credit card charges, including charges in respect of the 22 transactions, were discharged via automatic deduction from his bank account balance on 5 August 2024.

12 Unfortunately for the claimant, the 22 transactions with the relevant merchants were secured transactions, such that there were no chargeback rights as against the merchants. The respondent nevertheless offered to attempt to recover monies on a best-efforts basis but only succeeded in respect of two ICOCA transactions amounting to S$355.34, with such amounts credited back to the claimant.

The FIDReC adjudication

13 As for the remaining S$3,456.38 in respect of the remaining 20 transactions, the respondent considered that this loss should be borne by the claimant. The respondent did not accede to the claimant's request for a refund.

14 The case was referred to the Financial Industry Disputes Resolution Centre Ltd ("FIDReC"), and an adjudication was held on 23 July 2025. It is apposite to clarify at this juncture that adjudication is based on the terms of reference set by FIDReC regarding the process and outcome of adjudication, which both parties must agree to. The terms of reference expressly provide that the complainant (in this case, the claimant) is free to choose whether to accept the determination, and it is only if he accepts the determination that the financial institution (in this case, the respondent) is bound by such determination, and the parties would thereafter enter into a settlement agreement in accordance with the determination.

15 In other words, the outcome of the adjudication is more akin to the outcome of a neutral evaluation process that may assist parties to decide whether to enter into a settlement agreement. If the outcome is adverse to the complainant, he can choose not to accept and bring the dispute to another forum.

16 I was given to understand that the outcome of the adjudication process had been given on 28 July 2025 and was not in the claimant's favour, although I was not provided a copy of the grounds of decision. Dissatisfied with the outcome, the claimant did not accept the determination and commenced the present action on 25 November 2025.

Decision

Whether the claim falls within the jurisdiction of the Small Claims Tribunals

17 At the outset, I must clarify that the present claim arose from the contractual relationship between the claimant and respondent concerning the credit card services provided by the respondent. The claim therefore, in my

view, falls within the subject-matter jurisdiction of the tribunal, being one relating to a contract for the provision of services.

18 No arguments were advanced by the parties to suggest otherwise. Yet I note that there may be some concern regarding contracts relating to the provision of payment services, and whether Parliament intended for claims arising from such contracts to fall within the ambit of this tribunal's jurisdiction. This concern springs from paragraph 2 of the Schedule to the Small Claims Tribunals Act 1984 (2020 Rev Ed), which expressly deems contracts to buy or sell foreign currency notes with a licensed money-changing service provider under the Payment Services Act 2019 (2020 Rev Ed) (the "PSA") as contracts for the provision of services. Notably absent is any equivalent deeming provision for other payment services provided by licensed service providers under the PSA.

19 The question that presents itself is whether the absence of equivalent deeming provisions for other payment services means that the tribunal finds itself without jurisdiction over such matters. Such payment services would encompass the very credit card services provided under the contract between the parties in the present claim. This is so because payment services under the PSA embrace "account issuance services", which include the service of issuing a "payment account" and any services relating to the operation of such an account to any person in Singapore (see paragraph 3 of the First Schedule to the PSA). The term "payment account" is in turn defined under section 2(1) of the PSA to include a "credit card".

20 In my view, whilst the specific parliamentary purpose underlying paragraph 2 remains somewhat obscure, the proper interpretation is that this provision does not constrain the ordinary understanding of what constitutes a

service contract. Rather, it merely serves to clarify—perhaps out of an abundance of caution—that money changing falls within the category of service contracts. Had Parliament intended to circumscribe the rights of persons to bring claims for breach of service contracts, it would have provided clear and unambiguous language to that effect instead of speaking in riddles.

Whether liability for the 20 transactions should be borne by the respondent

The applicable liability apportionment framework

21 It was common ground that the 20 transactions were to be considered unauthorised credit card transactions, in that the claimant could not be regarded as having given authorisation or consent for such transactions to have been incurred. Further, it is undisputed that these transactions were likely made by an unknown scammer who had successfully added the claimant's credit card to the digital wallet of an Apple device.

22 Both parties further agreed that liability apportionment for such unauthorised transactions was to be governed by clause 13.4 of the credit card agreement between them. The relevant portions of this clause provided as follows:

> The Cardmember will not be liable for any unauthorised Card Transactions made after notification to the Bank and the liability will be limited to S$100 for any unauthorised transactions made before notification. If, however, it is found that the Cardmember has acted fraudulently, was grossly negligent or failed to inform the Bank of the lost or stolen card as soon as reasonably practicable then the Cardmember will be liable for all unauthorised transactions or amounts up to the Credit Limit (whichever is lower) and any additional interest, charges and late fees charged by the Bank...

23 The liability apportionment framework set out in this clause is based on the Code of Practice for Banks – Credit Cards issued by the Association of

Banks in Singapore ("ABS"), which prescribes the standards of service and conduct expected of ABS member banks, including the respondent.

24 Under this framework, liability for unauthorised transactions made prior to notification to the bank is ordinarily shared between the parties, with the cardholder bearing responsibility for a maximum of S$100 in total. This default apportionment yields, however, to a different regime where the cardholder has "acted fraudulently, was grossly negligent or failed to inform the Bank of the lost or stolen card as soon as reasonably practicable". In such circumstances, the burden of liability shifts entirely to the cardholder.

Parties' arguments

25 The respondent contended that the claimant acted with gross negligence and should therefore bear the full burden of these losses. The respondent did not rely upon the alternative grounds of fraud or failure to inform the respondent of a lost or stolen card as soon as reasonably practicable.

26 The respondent advanced three arguments to substantiate its allegation of gross negligence. First, that the claimant had disclosed his credit card details to the scammer. Second, that he had facilitated the tokenisation of his credit card to the scammer's digital wallet by disclosing the one-time password issued by the respondent—a disclosure that proved essential to completing the tokenisation process. Third, that despite receiving multiple SMS notifications from the respondent alerting him to the tokenisation activity and expressly instructing him to contact the bank if such steps were unauthorised, the claimant had not taken any remedial action.

27 The claimant, in response, said that he recalled attempting to purchase an item through an advertisement encountered while browsing TikTok, which

prompted him to enter his credit card details. Whether this constituted a phishing scam, he was unable to say with certainty. He maintained steadfastly, however, that he had not disclosed his one-time password to anyone. The SMS containing this password arrived at 11.13pm on 4 June 2024—a time when, according to the claimant, he would have been in his bedroom preparing for sleep, with his mobile phone remaining in the living room. As for the bank's subsequent notifications, the claimant acknowledged receiving them but explained that he ignored them entirely, reasoning that he was not a user of Apple Pay and therefore assumed they had no relevance to his circumstances.

Whether the claimant was grossly negligent

28 On the evidence before me, I found it more probable than not that the claimant did indeed disclose both his credit card details and the one-time password to the scammer, having fallen victim to a phishing operation.

29 While no direct evidence establishes this disclosure with certitude, such an inference represented the most natural and probable explanation for the sequence of events that unfolded. Without both the credit card details and the one-time password, the scammer would have been unable to successfully tokenise the claimant's credit card onto their Apple device. Yet the scammer accomplished precisely this feat at 11.14pm on 4 June—shortly after the one-time password was transmitted exclusively to the claimant via SMS. I was therefore satisfied that the claimant inadvertently disclosed the password to the scammer. I considered this to be more likely than the alternative scenario—that is, his mobile device had otherwise been compromised in some fashion, which would itself raise serious concerns about his digital security practices.

30 That said, I did not consider that the mere disclosure of credit card details and a one-time password through falling victim to a phishing scam necessarily constitutes gross negligence in every case.

31 It would be helpful at this juncture to examine more closely the concept of gross negligence, given that a finding must be made upon it. Negligence as a concept embodies a moral judgment about culpability, recognising that individuals may be held blameworthy for their failure to take reasonable care in engaging with considerations that ought to have guided their conduct. A person acts negligently when he fails to attend to considerations that a reasonable person would have recognised as material to the decision at hand, and where such failure to engage with those normative considerations reflects moral shortcomings on his part.

32 Gross negligence, in this regard, denotes a significantly higher degree of culpability than ordinary negligence: see *Red Sea Tankers Ltd v Papachristidis (The Hellespont Ardent)* [1997] 2 Lloyd's Law Rep 547 at 586. In my view, the distinction between ordinary and gross negligence emerges from a careful examination of two complementary assessments. The first involves identifying what considerations the person ought reasonably to have engaged with given their circumstances. The second requires evaluating the degree to which the individual's conduct fell short of reasonable expectations in failing to engage with those guiding considerations.

33 These inquiries demand careful attention to the full constellation of circumstances surrounding the individual's actions. Among the most salient considerations are the gravity and likelihood of the potential harm that might flow from the conduct, the obviousness of the risks involved, and whether the conduct violated well-established precautionary principles that, if properly

observed, would have prevented the harm in question. A person who ignores an obscure or remote risk occupies a different moral position from one who turns a blind eye to an obvious danger of serious and immediate harm.

34 In the final analysis, whether any particular course of conduct rises to the level of gross negligence must rest upon the specific facts of each case, examined with care and precision. No mechanical formula can capture the nuanced moral judgments that this standard requires.

35 Returning to the present context of unauthorised credit card transactions, phishing scams have grown increasingly sophisticated in recent years, employing techniques that may deceive even reasonably cautious individuals. Their risks and dangers may not always be readily apparent—even to a person exercising reasonable care. I would not, therefore, endorse any categorical proposition that falling victim to a phishing scam invariably constitutes negligence, much less gross negligence. Such a determination must depend upon the circumstances of each case, examined with appropriate sensitivity to the realities of modern digital fraud.

36 In the present case, absent evidence concerning precisely how the claimant came to divulge his credit card details and one-time password, I could not conclude on this basis alone that he had acted negligently, let alone with gross negligence.

37 However, I did find that a reasonable person in the claimant's position would have undertaken three essential steps upon receiving the respondent's notification alerts. First, he would have monitored such alerts in a timely manner, recognising their potential significance for his financial security. Second, he would have reported any unauthorised activity as soon as practicable

after receiving notification of suspicious conduct. Third, where circumstances warranted, he would have taken immediate steps to block further unauthorised access upon discovering that his credit card had been or appeared to have been compromised.

38 The notification alert transmitted to the claimant on 4 June made the situation unmistakably clear. The message stated that a one-time password had been requested to add his card to Apple Pay:

> Do not share your One-Time Password (OTP) with anyone. Use this OTP [redacted] to add your card ending [redacted] to Apple Pay within 3 minutes. If unauthorised, contact us: [redacted]

39 This message should have sounded the loudest of alarm bells, given that the claimant did not initiate the tokenisation process on Apple Pay. The communication explicitly warned that if this activity was unauthorised, he should contact the respondent immediately. He did not do so. Shortly thereafter, the claimant received a second alert confirming that his credit card had been successfully tokenised—constituting a second, unmistakable warning of potentially unauthorised activity:

> Thank you. You have tokenised your [redacted] card ending [redacted]. You can now use it to make purchases.

40 The warnings did not cease there. Further alerts followed on 6 June and 12 June respectively, each containing additional notifications concerning the tokenisation of his credit card to Apple Pay. In particular, the message of 6 June again emphasised in clear terms that if the card addition was unauthorised, he should contact the respondent.

41 When a cardholder has not initiated the tokenisation process himself, these alerts serve a critical function: they signal that someone unauthorised has obtained what amounts to a digital key to the cardholder's credit card details

and stands ready to employ it for conducting transactions that will be charged to the cardholder's account. This presents an obvious and serious risk of substantial financial harm. I accepted the claimant's explanation that the initial messages of 4 June arrived late at night, well past 11.00pm, and that he had not noticed or read them with appropriate care at that particular moment. But prudence and reasonable care demanded that he monitor these critical communications and took appropriate remedial action the following morning. He had not done so then, nor did he act upon the two subsequent opportunities that presented themselves to him over the following days.

42 In my judgment, the claimant had failed to attend to these obvious and significant risks across multiple opportunities, and to take steps to mitigate them in a timely manner despite having been alerted to such suspicious activity. Absent any reasonable explanation by the claimant, his pattern of inaction cannot be characterised as a mere oversight or momentary lapse in judgment. Rather, it represented a sustained course of omissions that fell significantly below the standard of reasonable care as to constitute gross negligence. This prolonged inaction subsequently enabled the scammer to employ the claimant's tokenised credit card through Apple Pay from 17 June onwards, executing the very unauthorised transactions that form the subject matter of this dispute.

43 Accordingly, the respondent was fully entitled to hold the claimant liable for the complete extent of losses arising from these unauthorised transactions, in accordance with the express terms of their credit card agreement.

Conclusion

44 For the foregoing reasons, I dismissed the claim. That said, the claimant's loss from this phishing scam warrants sympathy. The sum at stake represented a not insubstantial amount, and his confusion about how these

events came to pass is entirely understandable, given the relentless pace of technological evolution within an already complex industry of financial services, coupled with the ever-increasing sophistication of financial scams that prey upon ordinary consumers.

45 For lay users attempting to navigate this landscape, vigilance becomes essential. This vigilance must manifest itself in multiple forms: vigilance in monitoring and exercising appropriate care in online transactions, vigilance in protecting one's personal financial information from those who would misuse it, and perhaps most critically of all, vigilance in monitoring notification alerts from banks and financial institutions so that early intervention remains a viable possibility when suspicious activity occurs. When one encounters alerts whose significance remains unclear or mysterious, the prudent course invariably lies in seeking immediate clarification from the relevant institution rather than simply ignoring such communications and hoping for the best.

Joel Tan
Tribunal Magistrate

The claimant in person;
The respondent in person.