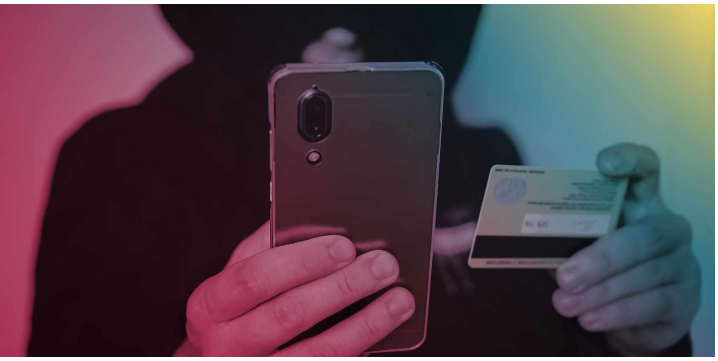
3-2021

Fraudulent transactions in an online world

Eunice CHUA
Singapore Management University, eunicechua@smu.edu.sg

Beverly WEE

LAW GAZETTE



FEATURE - February 2021

Fraudulent Transactions in an Online World

10min read
by Eunice Chua and Beverly Wee

This article considers the new normal of online payment transactions and the guidelines applicable to the situation of a fraudulent transaction. How effective are they at protecting consumers? Are there concerns that need to be addressed?

Electronic Payment as the New Normal

The use of electronic payments has grown over the years as an increasing number of consumers appreciate the convenience and rewards that come with such payments. Common forms of electronic payment include Visa PayWave and MasterCard PayPass, which are functions that credit and debit cards offer to allow purchases simply by waving the card at a contactless reader. Any transaction below S$200 can be processed in this way without the requirement of a PIN or signature to verify the transaction. [1] Electronic payments also include device-based digital wallets such as Apple Pay, Samsung Pay and Google Pay that allow purchases through a mobile phone's near field communication ('NFC') technology. Digital wallets may be internet based as well, with examples including PayPal, GrabPay, PayLah! and AliPay.

A research study published in October 2019 expected digital payments in Southeast Asia to exceed USD 600 billion in 2019 and reach USD 1 trillion by 2025. [2] Visa's Consumer Payment Attitudes Study conducted in October 2019 showed contactless payments on the rise in Singapore, with 84 per cent of consumers using this mode of payment. [3] Generation Y respondents are even higher at 92 per cent. The same study reported that almost half of consumers in Singapore carry less cash in their wallets as compared to 2018, with 68 per cent citing increased use of contactless payments as the reason for this change.

This electronic payment trend has been accelerated by the COVID-19 pandemic. As businesses have digitalised to stay afloat or seize new opportunities, consumers have embraced electronic payment methods that have allowed them to carry on transacting despite having to stay home or comply with safe distancing measures. [4] Some merchants now only accept contactless payment methods to the exclusion of all others.

Convenience Comes with Certain Risks

While electronic payments offer convenience and are effortless to carry out, they also come with risks. These include the risks of having one's account compromised due to ignorance, negligence, security breach or even fraud. To mitigate these risks, card associations such as Visa and MasterCard have implemented security measures like 3-D Secure ('3DS') to offer better protection for consumers. When at the checkout page of a 3DS merchant site, consumers will see a Verified by Visa

('VBV') or MasterCard SecureCode ('MSC') logo. Consumers will be prompted to input an OTP to authenticate the transaction. [5] The OTP is automatically generated via SMS to the cardholder's mobile phone and valid for only one unique transaction on a digital device. Thus, VBV/MSC provides additional security in two ways: first, as only legitimate commercial entities are able to offer the VBV/MSC service, consumers transacting with these merchants have some assurance that they are genuine; second, by requiring the keying in of an OTP that is sent only to the registered mobile phone of the cardholder, the cardholder is able to prevent an unauthorised payment by keeping the OTP secure. [6]

Nevertheless, many are still falling prey to scams that result in unauthorised and fraudulent transactions. This may be due in part to widespread accessibility to banking services in Singapore. As of 2020, 98 per cent of Singaporeans have bank accounts and 85 per cent of Singaporeans have credit cards. [7] Being a country that is digitally connected also makes Singapore more susceptible to online crimes. It was reported in 2020 that cybercrimes, and particularly scams, rose to 9,502 cases in 2019. [8] This constituted 27 per cent of the overall crime in 2019 and represented an increase of 53.5 per cent from the previous year. The total loss from the top ten scams was S$168.1 million; an increase of S$23.2 million from 2018. These scams included fraudulent transactions made with credit or debit cards, unauthorised access of an individual's online accounts and phishing e-mail scams. Another report highlighted that in 2019, more people were tricked into divulging their One-Time Password ('OTP') to scammers for online transactions than the previous year, with 1,101 victims losing around $15.3 million. [9] This compared with 244 victims being cheated of about $456,000 in 2018.

A Framework for Understanding Fraudulent Transactions

Such fraud may be broadly classified into two categories: authorised fraud and unauthorised fraud. Authorised fraud occurs where fraudsters trick individuals into transferring money to them or entering into other transactions that benefit the fraudsters. Take the example of a fraudster impersonating a government agency and calling someone to ask for details of their bank accounts. When the individuals realise that they have been scammed and seek the bank's help in retrieving the funds or for compensation, they often meet with obstacles because the bank will point out that the individual had in fact authorised the payment through providing an OTP and there was no wrongdoing on the part of the bank. Where fraud is authorised, it may be difficult for consumers to recover any compensation from their financial institution.

As for transactions made where the credit/debit card used is not present, 3DS authentication comes into play. For example, when a cardholder makes a purchase online, 3DS would prompt the cardholder to enter some form of password which could also be an OTP. By doing so, the transaction is authenticated and deemed authorised. Accordingly, where a merchant is enabled for 3DS authentication, it is no longer liable for certain fraudulent chargebacks where a cardholder claims that they did not make that purchase. [10]

In unauthorised fraud, the transfer of funds is processed by the fraudster and the individual does not provide any authorisation. This could take place through hacking or other criminal activity, such as stealing and using a credit or debit card with contactless payment functions, making online purchases with a stolen or lost credit or debit card from merchants who do not use 3DS, and counterfeiting cards. In such situations, although the customer does not authorise the transaction, recovery is nevertheless not a given because the consumer remains responsible to take steps to mitigate the loss.

The Position in Singapore

Despite the prevalence of fraudulent transactions, there is very little in hard law that clearly sets out the rights and responsibilities of the individual consumer, the financial institution and any other intermediaries in the transaction. Rather, the position in Singapore has been left largely to soft law and practice. All these also appear limited to unauthorised fraud, suggesting that authorised fraud remains the responsibility of the consumer.

Where credit cards are involved, under a Code of Practice issued by the Association of Banks in Singapore ('ABS'), cardholders are able to limit their maximum liability for fraudulent transactions in the following terms:

> "Prior to notification of credit card loss to card issuers, the maximum liability for cardholders due to unauthorised charges is $100 unless the cardholder has acted fraudulently, or has been grossly negligent, or has failed to inform the card issuers as soon as reasonably practicable after becoming aware that his or her card has been lost or stolen." [11]

This standard has made its way into the cardholder agreements of various banks albeit with some variation in language that is often less favourable to the consumer. For example, instead of "as soon as reasonably practicable", cardholder agreements may require "immediate" notification. Instead of using when a consumer becomes aware of the loss or theft of the card as a starting point, cardholder agreements may refer to when a consumer receives any transaction notification alert. Instead of disclaiming liability when a consumer has been "grossly negligent", the cardholder agreement may do so as long as the consumer has been simply "negligent" as determined by the bank.

As for other types of electronic payment transactions, which includes stored-value facilities such as GrabPay, Singtel Dash, EZ-Link and Nets, [12] the Monetary Authority of Singapore ('MAS') has issued Guidelines that allow the account holder to disclaim liability for any:

> "loss arising from an unauthorised transaction that does not exceed $1,000, if the loss arises from any action or omission by any third party [excluding the responsible financial institution, its employee, its agent or any outsourcing service provider] and does not arise from any failure by any account user to comply with any duty in Section 3." [13]

Section 3 of the Guidelines details the duties of account holders, which include providing contact details to the relevant financial institution, opting in for and monitoring all notifications, keeping all account access code private, and reporting any unauthorised transactions "as soon as practicable" [14] . These Guidelines are fairly new, but do not appear to be widely incorporated.

Concerns that Arise Out of the Existing Situation in Singapore

It would be evident that although there are some key themes that emerge, for example that the card holder or account holder has a responsibility to notify the financial institution within a very short period of time, to safekeep access codes, and monitor transactions and notifications, there is very little light shed on the responsibility of the financial institution.

Does the financial institution have any responsibility towards the consumer in terms of fraud detection and identifying transactions that are unusual given the consumer's usual pattern of behaviour? Is it sufficient for the financial institution to send out notifications and statements and leave it to the consumer to sound out? Is the financial institution required to assist the consumer to apply for a chargeback or reversal from the card company or merchant? These appear all to be left to contractual arrangements and the different practices of the financial institutions.

Even with the ABS Code of Practice and MAS Guidelines, there is inconsistency in their implementation and little recourse for the consumer who will be contractually bound by the precise terms and conditions that their financial institution imposes. As mentioned above, different banks have through their respective cardholder agreements created differing

standards as to the level of care required on the part of the consumer, and how much time the consumer has to notify them of the fraudulent transaction. The banks have also accorded to themselves the discretion to determine whether a consumer has behaved negligently, without giving clear information as to what may constitute negligence. All these have a significant impact on determining whether the consumer may successfully limit their liability for the fraudulent transaction.

As between the ABS Code of Practice and the MAS Guidelines, different frameworks have also been created for credit cards and other electronic payment transactions. The guidelines set out by MAS allows the accountholder to claim up to $1,000 while ABS limits the cardholder's liability to $100. Specific responsibilities that accountholders should comply with are clearly indicated in the same set of guidelines by MAS. Such duties include how an accountholder can protect access to the account and the importance of enabling transaction alerts. On the other hand, ABS plainly states that the transaction should not arise from fraudulent and/or negligent acts and that one should report immediately. In brief, both organisations set out similar requirements, i.e. the loss shall not be due to the accountholder/cardholder's negligent and/or omission, but differ in the details. Yet, credit cards and other electronic payment transactions may well overlap in practice. For example, payment methods may be combined in the following ways:

- A credit card is used to top up stored-value facilities such as EZ-Link and another transaction is made using EZ-Link.
- A transaction is made through PayPal with credit card details keyed in on PayPal's portal.
- Other digital payment/e-wallets such as Apple Pay, Samsung Pay, GrabPay may be funded by credit cards.

Where the fraudulent transaction is made through combined means, the account holder may not know whether they can rely on the ABS Code of Practice or the MAS Guidelines.

From the consumer's perspective, all this is confusing and may not square with their expectations. A consumer may not appreciate what standard of behaviour is required especially as these are not consistent between the ABS Code of Practice and the MAS Guidelines. A consumer may also not understand why authorised fraud is treated differently from unauthorised fraud when in both situations he or she is a victim. A consumer holding multiple credit cards with differing terms may face different outcomes from different banks depending on the precise terms of the cardholder agreement each has. He or she may not understand why this should be the case as a matter of principle. The lack of clarity on the obligations of a financial institution may also breed unrealistic expectations on the part of the consumer, who may expect the financial institution to be liable for the fraudulent transaction as the card issuer should have detected the fraud and prevented the transaction from going through in the first place.

All this points towards the need for clearer standards and for these to be communicated to the public at large.

Conclusion

It may be beneficial for the regulator and financial institutions to come together to consider a more standardised approach alongside structural changes to the payments system for the ease of the industry and its consumers.

In the UK, a "Contingent Reimbursement Model" Code was entered into voluntarily by UK Banks in May 2019. This was an initiative by the UK payments industry that is focused on compensating those who have suffered from authorised push payment fraud and where applicable. The code states that victims of authorised push payment scams, which take place when customers transfer money directly to fraudsters who are impersonate someone the victim trusts, "should" be reimbursed, unless they ignore warnings from their bank or were grossly negligent. This contrasts with the current position in Singapore where a victim of authorised fraud is usually unable to recover from the financial institution on the basis they authorised the transaction.

In terms of structural changes to the payments system, the UK also provides a model for consideration. From July 2020, "confirmation of payee" came into force in the UK. [15] This was a method designed to provide verification of the intended recipient to account holders who wished to send payment. This was done with the aim of reducing fraudulent transactions and misdirected payments by making it more difficult for fraudsters to mask themselves. Malaysia has also since moved away from signature verification cards and implemented a PIN-based card system to provide better protection against fraudulent transactions.

Implementing a standard procedure and standardised approach may be advantageous as this may be more comprehensible to the general public, which may in turn lead to fewer disputes. The values of these disputes do not often justify formal legal proceedings and consumers often turn to the Financial Industry Disputes Resolution Centre ('FIDReC') for assistance. A growing proportion of FIDReC's complaints against banks and finance companies stem from fraudulent transactions. This increased from 23 per cent in 2017/2018, to 26 per cent in 2018/2019 to 29 per cent in 2019/2020. However, as an alternative dispute resolution provider, FIDReC has limited powers to address the larger-scale problems faced by consumers discussed in this article. Ultimately, prevention is better than cure and hence consumer education could lead to more responsible cardholders who better understand their obligations as users of electronic payments. It is hoped that lawyers, being the first port of call when a dispute arises, will be able to contribute to such education efforts as well.

Endnotes

This transaction limit was recently revised from $100, see Press Release, “More than Half of Singaporeans Use Mobile Contactless Payments: Visa Study”, 28 May 2020, available online: <https://www.visa.com.sg/about-visa/newsroom/press-releases/more-than-half-of-singaporeans-use-mobile-contactless-payments-visa-study.html> (last accessed 25 January 2021).

Google, Temasek and Bain & Company, “e-Conomy SEA 2019”, p 46, available online: <https://www.blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf> (last accessed 25 January 2021).

Press Release, “More than Half of Singaporeans Use Mobile Contactless Payments: Visa Study”, 28 May 2020, available online: <https://www.visa.com.sg/about-visa/newsroom/press-releases/more-than-half-of-singaporeans-use-mobile-contactless-payments-visa-study.html> (last accessed 25 January 2021).

Vivienne Tay and Rachel Mui, “Contactless payment options on the rise amid Covid-19 outbreak”, *Business Times* (26 June 2020); Hariz Baharudin, “Addendum to President’s Address: Singapore to continue investing in technology and innovation to fuel growth”, *Straits Times* (26 August 2020).

See The Association of Banks in Singapore website, “Consumer Banking \ FAQ For Consumers \ Payment Card Security”, <https://www.abs.org.sg/consumer-banking/consumers/payment-card-security> (last accessed 25 January 2021).

https://www.sc.com/bn/ways-to-bank/3d-secure-faq> (last accessed 25 January 2021).

Diego de Sartiges et al, “Southeast Asian Consumers are Driving a Digital Payment Revolution”, *Boston Consulting Group* (20 May 2020), available online: <https://www.bcg.com/en-sea/publications/2020/southeast-asian-consumers-digital-payment-revolutions> (last accessed 25 January 2021).

Overseas Security Advisory Council, “Singapore 2020 Crime & Safety Report”, 4 June 2020, available online: <https://www.osac.gov/Country/Singapore/Content/Detail/Report/7f0cc2bc-ba9b-4485-b58b-1861aa0f8fc3> (last accessed 25 January 2021).

Cara Wong, “More fall for OTP scams, lose over $15m”, *The Straits Times* (2 April 2020), available online: <https://www.straitstimes.com/singapore/courts-crime/more-fall-for-otp-scams-lose-over-15m> (last accessed 25 January 2021).

Worldpay Developers, “Liability Shift For Cards”, n.d., available online: <https://developer.worldpay.com/docs/wpg/reference/liabilityshift> (last accessed 25 January 2021).

The Association of Banks in Singapore (ABS), “Code of Practice for Banks – Credit Cards”, p 3, 2 July 2020, available online: <https://www.abs.org.sg/docs/library/code-of-practice-for-banks—credit-cards.pdf> (last accessed 25 January 2021).

Irene Tham, “Consumers can set own limits for e-payment alerts”, *The Straits Times*, (26 April 2019), available online: <https://www.moneysense.gov.sg/-/media/moneysense/media-article/consumers-can-set-own-limits-for-e-payment-alerts.pdf> (last accessed 25 January 2021).

Monetary Authority of Singapore, “E-Payments User Protection Guidelines”, p 17, 5 September 2020, available online: <https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Payment-and-Settlement-Systems/PSOA-Guidelines/E_payments-User-Protection-Guidelines-WEF-5-September-2020.pdf> (last accessed 25 January 2021).

Ibid, p 7 – 10.

Payment Systems Regulator, “PSR Confirms Widespread Implementation Of Name-Checking System, Confirmation Of Payee”, 1 July 2020, available online: <https://www.psr.org.uk/news-updates/latest-news/announcements/psr-confirms-widespread-implementation-of-name-checking-system-confirmation-of-payee/> (last accessed 18 December 2020).

Tags: ALTERNATIVE DISPUTE RESOLUTION, CONSUMER PROTECTION, FINANCIAL SERVICES AND REGULATION, ONLINE PAYMENTS, UNAUTHORISED PAYMENTS

Eunice Chua

CEO, Financial Industry Disputes Resolution Centre
Research Fellow, Singapore International Dispute Resolution Academy, Singapore Management University School of Law

Beverly Wee

Manager (Alternative Dispute Resolution), Financial Industry Disputes Resolution Centre
E-mail: info@fidrec.com.sg