Are hackers outsmarting our banks in their security measures?

Description

A year ago, news first emerged that hackers may have found a new way to outsmart our banks in their security measures, even after they introduced their 2-FA authentication protocol where consumers would have to key in a One-Time Password (OTP) sent to their mobile phone whenever they make an online transaction using their credit card(s).

Their method? Just hack into the victims' mobile phone, where the hackers can then access both credit card details and OTPs at one go. Apps or websites where the consumer have previously keyed in their credit card information can reveal the card details, whereas the SMS would give the OTP required to make sure the transaction goes through.

I'm not making it up. Take a look at this case as reported by The Straits Times last year:

Mr Philip Loh had his phone hacked into and credit card details stolen last year, with six flight tickets costing $12,327 being bought in Eastern Europe. He appears to be the victim of a malicious program that the public was warned about last month. ST PHOTO: ALICIA CHAN

———

When he woke up on Sept 30 last year, his phone was still "updating". He forcibly rebooted it by removing the battery, only to find SMS alerts from UOB on the purchases, as well as the one-time passwords (OTPs) used to authenticate them.

Mr Loh appears to be one of the victims of a malicious program that the Association of Banks in Singapore (ABS) warned the public about last month. He insists he has entered his credit card details on his phone only twice or thrice in the past year – to buy movie tickets online.

He was told by the bank that one of the reasons the payments could not be waived was that they were made under the "3D secure payment system" – which authenticates online transactions by sending an OTP to the customer's cellphone. The Straits Times understands that because the hackers obtained the OTPs, the payment system was not compromised.

UOB said: "We review each customer dispute case thoroughly and take into account a number of contributing or mitigating factors. These include whether a customer had provided his credit card information on a phishing site or if transactions were authorised with an SMS OTP. In this present case, the bank's security measures were not compromised."

UOB is asking him to pay $5,000 of the $12,327, having reduced the amount out of goodwill, or it would take legal action.

Case executive director Seah Seng Choon said banks need to keep in mind shifting security vulnerabilities. "If a third party can hack into the system and perform transactions in this manner, it shows that the system needs to be reviewed to protect consumer interests."

Information technology lawyers said crooks are starting to get the better of two-factor authentication systems.

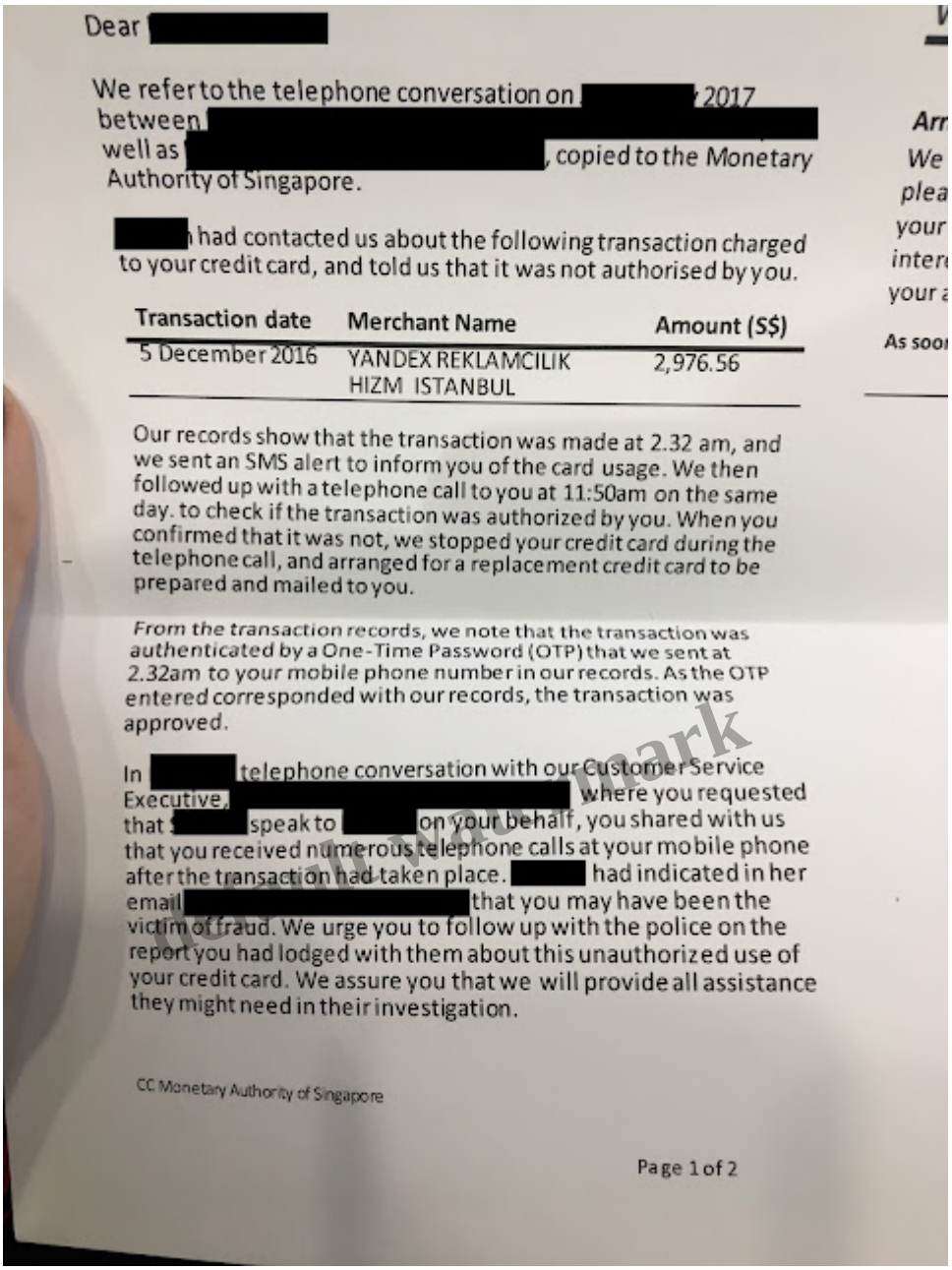
Source: Man in row with bank over hacked phone (The Straits Times)

———

A year on, have our local banks failed to do anything about this?

I would have thought that with this scam being made public and ABS having warned everyone, the banks would have already made steps to further strengthen their security systems and outwit the hackers. However, my friend was recently the victim of such a fraud case, which seems to be similar to Mr Loh's case…and OCBC basically told her to pay for a transaction she never made.

OCBC claims that the transaction was approved as the (OTP) provided matched the one that was sent to her mobile phone as part of their 2-FA protocol.



Dear [redacted]

We refer to the telephone conversation on [redacted] 2017 between [redacted] as well as [redacted], copied to the Monetary Authority of Singapore.

[redacted] had contacted us about the following transaction charged to your credit card, and told us that it was not authorised by you.

Transaction date	Merchant Name	Amount (S$)
5 December 2016	YANDEX REKLAMCILIK HIZM ISTANBUL	2,976.56

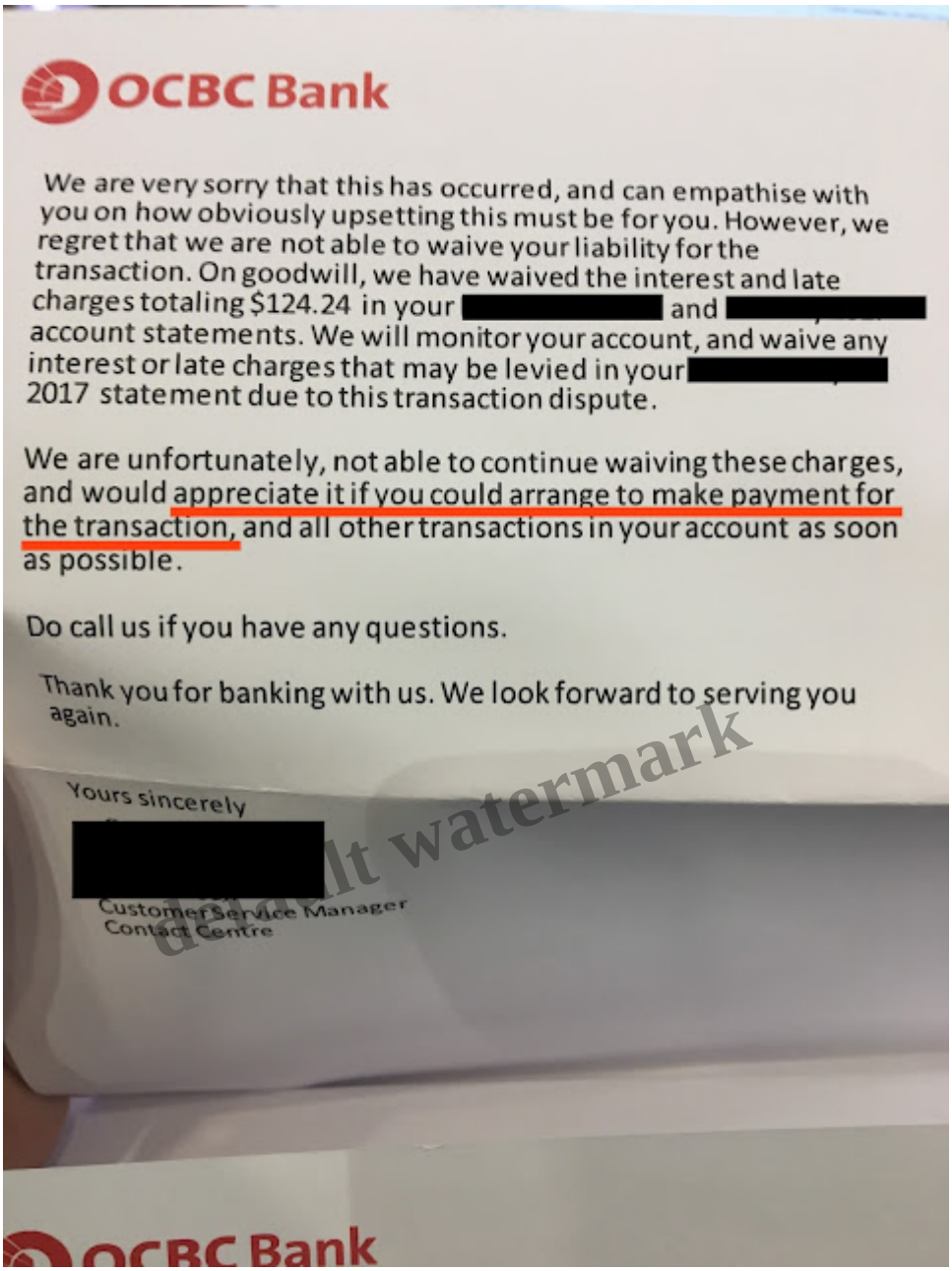
Our records show that the transaction was made at 2.32 am, and we sent an SMS alert to inform you of the card usage. We then followed up with a telephone call to you at 11:50am on the same day. to check if the transaction was authorized by you. When you confirmed that it was not, we stopped your credit card during the telephone call, and arranged for a replacement credit card to be prepared and mailed to you.

From the transaction records, we note that the transaction was authenticated by a One-Time Password (OTP) that we sent at 2.32am to your mobile phone number in our records. As the OTP entered corresponded with our records, the transaction was approved.

In [redacted] telephone conversation with our Customer Service Executive, [redacted] where you requested that [redacted] speak to [redacted] on your behalf, you shared with us that you received numerous telephone calls at your mobile phone after the transaction had taken place. [redacted] had indicated in her email [redacted] that you may have been the victim of fraud. We urge you to follow up with the police on the report you had lodged with them about this unauthorized use of your credit card. We assure you that we will provide all assistance they might need in their investigation.

CC Monetary Authority of Singapore

Page 1 of 2



Now, this worries me.

As consumers, we bank with our local banks believing their claims that their security systems are highly secure. But incidents like these clearly show that they are not. Furthermore, it shows that our banks have failed to keep up with the hackers even after their ways of outsmarting their security systems have been made known.

We're heading towards a cashless society, but what implications will that bring? While Paywave, Apple Pay, Android Pay and a whole load of other cashless technologies promise us convenience, at what cost will this come at?

Even when some folks were complaining about the 2-FA system being a hassle, I gladly welcomed it as I saw it to be a necessary hassle to prevent fraud whenever we transact online. However, now that I

know hackers can simply outsmart the system by hacking into our mobile phones, we may no longer be safe even with 2-FA authentication methods.

You might want to disable mobile apps that have your credit card details autosaved and clear your cookies / history as well if you want to prevent this from happening to you.

Any of us could be the next victim.

With love and concern,
Budget Babe

Category

1. Credit Cards
2. Savings