PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPC 2

Case No. DP-2011-B7409 / DP-2011-B7421

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012

And

Quoine Pte Ltd

… *Organisation*

DECISION

Quoine Pte Ltd

[2022] SGPDPC 2

Lew Chuen Hong, Commissioner — Case Nos. DP-2011-B7409 / DP-2011-B7421

8 February 2022

Introduction

1 On 17 November 2020, Quoine Pte Ltd ("**the Organisation**") informed the Personal Data Protection Commission ("**the Commission**") that its domain manager had transferred control of its domain hosting account to an external actor, who accessed and exfiltrated the personal data of 652,564 of its customers ("**the Incident**"). The Commission subsequently received a complaint from an individual believed to have been affected in the Incident.

2 The Organisation requested for the investigation to be handled under the Commission's Expedited Breach Decision procedure. In this regard, the Organisation voluntarily provided and admitted to the facts set out below, and admitted that it had failed to implement reasonable security arrangements to protect the personal data accessed and exfiltrated in the Incident in breach of Section 24 of the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

3 The Organisation is a company incorporated and based in Singapore, and a subsidiary of Liquid Group Inc., which is incorporated in Japan. The Organisation operates a global cryptocurrency exchange under the "Liquid" brand, and has customers around the world.

4 At the time of the Incident, the Organisation's back-end IT infrastructure included the following:

(a) Its vendor-procured cloud computing platform ("**Cloud Platform**") which it used to run its cryptocurrency exchange platform, and which hosted its cloud computing database; and

(b) Its additional cloud computing storage procured from another vendor, which it used to store documents such as Know-Your-Client ("**KYC**") documents.

5 The Organisation also engaged a third party domain name registrar ("**the Domain Provider**") to register and host the Organisation's domain (@quoine.com domain). A domain name registrar allows a party to purchase and register domain names, where the domain name translates to a public address of the party's servers (e.g. webserver, email server) for routing purposes.

6 On 13 November 2020, a staff member of the Organisation received an email from the Domain Provider stating that changes had been made to the settings of the Organisation's domain hosting account with the Domain Provider (@quoine.com domain) ("**Domain Hosting Account**"). Staff members also received password reset emails for accounts on the Organisation's other file-sharing and office productivity services. As the Organisation had not requested for the changes, the Organisation followed up with the Domain Provider, who acknowledged that the Organisation's email accounts on its domain with the Domain Provider were no longer routed to the Organisation.

7 Investigations revealed that:

(a) As a result of social engineering attacks on employees of the Domain Provider, an employee of the Domain Provider incorrectly transferred control of the Organisation's Domain Hosting Account to an external actor. This allowed the external actor to change the registered email address on the Organisation's Domain Hosting Account and subsequently effect a password reset on the account to take control of the Domain Hosting Account.

(b) Control of the Domain Hosting Account allowed the external actor to know the number of servers using the domain name, and the IP addresses of these servers.

(c) With control of the Domain Hosting Account, the external actor changed the servers to which the Organisation's email traffic was directed (i.e. via changes to the Organisation's mail exchanger (MX) records), from the email servers used by the Organisation to the external actor's email servers. This redirected all of the Organisation's emails to the external actor's email servers. According to the Organisation, this impacted the Organisation's security monitoring capability as many alerts and notifications, which were distributed via email, were consequently redirected to the external actor's email servers. The Organisation's staff members continued to receive emails notifying of changes to the settings of the Domain Hosting Account (referred to at [6] above) on alternative recovery options that had been set up.

(d) Having redirected the Organisation's emails on the Organisation's domain (@quoine.com domain) to itself, the external actor then initiated password resets for several of the services tied to the Domain Hosting Account. The external actor successfully carried out a password reset on an account ("**DevOps Account**") used by the Organisation for automation tasks and to run codes throughout the day which was not used interactively by humans.

(e) The external actor then used the DevOps Account's newly reset credentials to access the Organisation's Cloud Platform, which hosted API keys/token to the Organisation's database hosted within the Cloud Platform as well as a separate cloud computing storage database (collectively, the "**Databases**"). The external actor thereby gained credentials to the Databases, and accessed and exfiltrated personal data stored in the Databases.

8 The personal data of 652,564 of the Organisation's customers was accessed and exfiltrated in the Incident, comprising the following:

(a) First name and surname;

(b) Address;

(c) Email address;

(d) Telephone number (optional);

(e) Photo-image of documents provided by 362,035 customers for KYC purposes before 13 October 2018, namely, NRIC number, passport number or other identification documents, proof of address document, and photograph;

(f) Financial information of Japanese customers of Quoine Corporation, a Japanese company related to the Organisation;

(g) Transaction information: fiat deposits and crypto withdrawals, and a 2018 record of balances prior to the launch of the current "Liquid Exchange"; and

(h) For customers depositing and withdrawing fiat currencies: Bank account and other information, namely, name of the bank, account number and name of the account holder.

(collectively, the "**Customer Data**").

Remedial actions

9 Following the Incident, as part of remedial actions, the Organisation:

(a) Notified its customers to alert them of the Incident, advised them of actions to take to secure their accounts, and recommended precautionary measures to monitor any suspicious activities which may have suggested improper use of their personal information;

(b) Moved its domains to a more robust service provider that offered Enterprise level support, strong access control (username, password and mandatory two-factor authentication ("**2FA**")) and roles-based access controls;

(c) Migrated the entire Liquid exchange to a different vendor-provided cloud computing platform, with additional improvements made in the interactions between the Organisation's service accounts and the system; and

(d) Strengthened the use of the DevOps Account, and imposed IP whitelist restrictions where appropriate.

10 The Organisation is also evaluating other services to further harden its infrastructure, including cloud security configuration tools.

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation

11 Section 24 of the Personal Data Protection Act 2012 ("**PDPA**") requires an organisation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

12 As a preliminary point, while the Organisation had engaged the Domain Provider to host the Organisation's domain, the Domain Provider did not process any personal data on behalf of the Organisation and was not the Organisation's data intermediary. Due consideration is given to the fact that the initial breach occurred with the Domain Provider. The basis of the Commission's decision is that the Protection Obligation in respect of the Customer Data was borne solely by the Organisation and there were failures in respect of how it secured access to its Cloud Platform, leading to the unauthorised disclosure of Customer Data.

13 The Commission has repeatedly highlighted that an organisation should design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach, and implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity (see the Commission's Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised 1 October 2021) ("**Advisory Guidelines**") at [17.3]; see also *Credit Counselling Singapore* [2017] SGPDPC 18 at [25] and *PeopleSearch Pte. Ltd.* [2019] SGPDPC 47 at [10]). As stated in the Commission's Advisory Guidelines at [17.5], measures that an organisation can use to protect personal data include adopting appropriate access

controls (e.g. considering stronger authentication measures where appropriate) and installing appropriate computer security software and using suitable computer security settings.

14 Considering the Organisation's business as a global cryptocurrency exchange that regularly deals with a large volume of sensitive personal data of a financial nature, the Organisation's overall data protection and cybersecurity posture should have been very much heightened. The Organisation was in possession of 822,096 individuals' Customer Data, including photo-image of documents and other information provided by 362,035 customers for KYC purposes, cryptocurrency transactions and bank account information. Consequently, the Organisation is required under the Protection Obligation to have implemented strong security arrangements to protect the Customer Data held in its Databases.

15 In the present case, the Organisation has admitted that it failed to implement reasonable security arrangements to protect the Customer Data, and that it was in breach of the Protection Obligation. In particular, the Organisation (i) failed to review and assess the DevOps Account's security implications and risks, and (ii) failed to implement reasonable ICT controls for the DevOps Account.

Failure to review and assess the DevOps Account's security implications and risks

16 The Commission has highlighted in previous decisions the importance of carrying out correctly-scoped periodic security reviews, so as to detect vulnerabilities and assess security implications and risks, and to ensure that reasonable security arrangements have been put in place to protect personal data in an organisation's database.

17 In *WTS Automotive Services Pte. Ltd.* [2018] SGPDPC 26 ("***WTS***"), the Commission highlighted the importance of conducting regular reviews to ensure that websites collecting personal data and electronic databases storing personal data have "reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks", as personal data of individuals may be exposed if a website or database in which it is stored contains vulnerabilities (at [18] of *WTS*).

18 Likewise, in *Commeasure Pte Ltd* [2021] SGPDPC 11 ("***Commeasure***"), the organisation had neglected to include the affected application package and access key (which the threat actor had used to access and exfiltrate personal data in the organisation's cloud database) in its inventory of IT assets in production, which had resulted in their omission from its periodic security reviews. The organisation was found in breach of the Protection Obligation on this basis, as the vulnerability could otherwise have been discovered and the incident could have been prevented (at [16]-[17] of *Commeasure*). While the organisation explained that its failure to implement sufficiently robust processes to manage its inventory of infrastructure access keys was attributable to the high turnover of its employees from the time of its inception to the discovery of the incident, this was unacceptable because the organisation's responsibility to protect personal data in its control or possession ought not to have been subjected to staff movement or appointment (at [13] of *Commeasure*).

19 As held in *Chan Brothers Travel Pte Ltd* [2020] SGPDPCS 11 ("***Chan Brothers***"), organisations must be aware of security implications of software features of their IT systems, so as to configure the security settings to enable effective protection of personal data stored in the IT systems (at [5] of *Chan Brothers*).

20 During the investigations, the Organisation admitted that its periodic reviews of access "failed to acknowledge this weakness as they incorrectly focussed on accounts used interactively by humans only, and not the automation bot accounts". According to the Organisation, until the Incident, it was not aware of the vulnerability and weakness in access control to the DevOps Account, which did not have 2FA enabled. Accordingly, similar to the facts of *Commeasure* as set out above, although the Organisation had conducted periodic security reviews, these security reviews were improperly scoped, and failed to identify this vulnerability present in the DevOps Account.

21 The Organisation also admitted that the DevOps Account "was created without sufficient due diligence being given to the entire security risk profile of this type of account", and "[t]his is a vulnerability that had not been adequately assessed by implementing alternative security measures to address the lack of 2FA".

22 The Organisation had therefore failed to review and assess the security implications and risks arising from the DevOps Account and its lack of 2FA. The Organisation's failures in this regard were especially egregious, given that the DevOps Account had privileged access to the Organisation's Cloud Platform containing API keys/tokens to the Databases, and consequently, the Customer Data stored in the Databases. If the Organisation had included the DevOps Account in its security review and detected the vulnerabilities in the lack of 2FA, and/or had assessed and appreciated the security implications and risks arising from the DevOps Account and its lack of 2FA, it could have taken reasonable security measures to mitigate these security risks and to configure the security settings to enable effective protection of the Customer Data in the Databases.

23 The Organisation informed the Commission during the investigations that its current staff were not aware of the reasons for the DevOps Account's set-up and security arrangements, as the DevOps Account had been created "at some time in the past (so legacy)". The Organisation explained that there had been internal personnel movement. For instance, its DevOps team had initially been based in and managed out of Tokyo, then Quoine Vietnam. However, by mid-2020, the DevOps Tokyo team was no longer with the Organisation, and the DevOps team that remained was in Quoine Vietnam. While we are sympathetic to the challenges presented as a result of any personnel movements, it was incumbent on the Organisation to implement the necessary systems and processes to ensure that critical information about its IT systems, including legacy systems, survived the turnover of its staff. As the Commission has also held in *Commeasure* and stated above, an organisation's responsibility to protect personal data in its control or possession ought not to have been subjected to staff movement or appointment.

24 The Organisation suggested that the DevOps Account's security risk profile had not been assessed, probably due to its intended use as an automation account. This was not accepted. The Organisation is not exempted from assessing the security implications and risks of the DevOps Account simply on the basis that it was an automation account, especially considering that the DevOps Account could be used to access the Customer Data stored in the Databases.

25 In view of the above, the Organisation was found to be in breach of the Protection Obligation for its failure to review and assess the DevOps Account's security implications and risks.

Failure to implement reasonable ICT controls for DevOps Account

26 As stated in the Commission's Guide to Data Protection by Design for ICT Systems (2021), organisations should put in place ICT controls to manage data protection risks (at page 9). Examples of ICT controls include setting appropriate access control rules, access rights and restrictions for specific user roles, and strengthening database security (at pages 15 and 18).

27 The Organisation informed the Commission that 2FA had not been implemented for the DevOps Account, which had privileged access to the Cloud Platform containing API keys/tokens to the Databases, and consequently, the Customer Data stored in the Databases. This meant that the DevOps Account is an account with privileged access. Many of the Organisation's other systems and services had implemented 2FA for accounts with privileged access, and these were not breached in the Incident as the external actor could not carry out a password reset on these systems and services. In the present case, the external actor had been able to access the Cloud Platform and the API keys/tokens to the Databases stored therein, after carrying out password reset on the DevOps Account.

28 The Organisation could have guarded against this risk by strengthening ICT controls for the DevOps Account. The Organisation could have limited access to the password change functions of its DevOps Account. The Organisation could have introduced an additional restriction on the password change function, by requiring 2FA whenever there is a request to change passwords for the DevOps Account. The Organisation had implemented this additional restriction for many of its systems and services, which were not breached in the Incident as the external actor could not carry out a password reset where 2FA was required. The Organisation could likewise have implemented a 2FA requirement for effecting password resets for the DevOps Account. This was an existing policy and practice that the Organisation had for other

accounts with privileged access, and it ought to also have been extended to the DevOps Account which also had privileged access.

29 Accordingly, the Organisation was found to be in breach of the Protection Obligation for failing to implement reasonable ICT controls for the DevOps Account.

The Commissioner's Directions

30 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and the amount of any such financial penalty, the matters set out at section 48J(1) and the factors listed at section 48J(6) of the PDPA were taken into account, as well as the following mitigating factors:

Mitigating Factors

(a) The Organisation took prompt remedial actions, including notifying the affected individuals; and

(b) The Organisation was cooperative during investigations.

31 The Commission also considered the Organisation's voluntary acceptance of liability for the Incident.

32 Having considered all the relevant factors of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $67,000 within 30 days from the date of the relevant notice accompanying this decision, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

33 No further directions are necessary on account of the remedial measures already taken by the Organisation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION