Amicus Solutions Pte. Ltd. & Anor.

[2019] SGPDPC 33

Tan Kiat How, Commissioner — Case No DP-1610-B0290

Data protection – Consent obligation – Notification obligation -Unauthorised use of personal data

Data protection — Consent obligation – Notification obligation -Unauthorised sale of personal data

Data protection – Continued disclosure of personal data collected before appointed day

30 August 2019.

1 The Personal Data Protection Commission (the "**Commission**") received a complaint regarding the unauthorised collection and use of personal data to market financial products. Investigations were commenced into the alleged unauthorised sale and disclosure of personal data by a data broker and the unauthorised collection and use of the personal data for telemarketing purposes. Upon conclusion of investigations and consideration of the totality of evidence, the Commissioner found Amicus Solutions Pte. Ltd. ("**Amicus**") and Mr Ivan Chua Lye Kiat ("**Mr Chua**") to be in breach of the Personal Data Protection Act 2012 ("**PDPA**") for the reasons set out in these grounds.

Material Facts

2 An independent life insurance brokerage company (the "**Insurance Brokerage**") appointed Mr Chua as a financial adviser director to provide financial advisory services and to market financial products distributed by the Insurance Brokerage to prospective clients in accordance with the terms set out in a Financial Adviser Representative Agreement. He oversees a team of financial adviser representatives. Their main products are Eldershield related insurance policies targeted at individuals over 40 years old.

3 It is undisputed that Mr Chua and the financial adviser representatives in his team are not employees of the Insurance Brokerage but independent agents. As independent agents, they receive a commission for each sale but are not in an employer-employee relationship with the Insurance Brokerage nor are they entitled to any employee benefits such as employer Central Provident Fund contributions and/or medical benefits.

4 One of Mr Chua's primary roles as a financial adviser director is to seek out new customers. Mr Chua mainly relied on referrals from existing customers but he also engaged telemarketers to make cold calls to potential customers. These telemarketers are independently sourced with no assistance of or referrals from the Insurance Brokerage; telemarketers are directly engaged by Mr Chua or the financial adviser representatives in his team.

5 Amicus is an organisation that provides business and consultancy management services and claims to be able to provide business opportunities and marketing plans with its database. It claims to have 1.8 million contacts which it markets as being in compliance with the PDPA and the Personal Data Protection (Do Not Call Registry) Regulations 2013. Aside from the sale of data, Amicus also offers a range of services such as purchasing property

ownership information (including caveats) on behalf of property agents, data mining and Do Not Call ("**DNC**") Registry scrubbing services.

6 During investigations, Mr Chua was upfront in admitting that he had purchased telemarketing leads from Amicus both before and after 2 July 2014, the date when Parts III to VI of the PDPA ("**Data Protection Provisions**") came into effect (the "**Appointed Day**"). Mr Chua represented that before the Appointed Day, Amicus sold personal data (including the individual's name, mobile number, gender and birthday) at S$0.50 to S$1.00 per record. After the Appointed Day, the products that were offered by Amicus changed. The previous product was no longer offered but it now offered different products. For Mr Chua's commercial purposes, the product that he was interested in was the sale of telephone numbers of individuals above 40 years old (which was his team's target demographic), each of which was sold for between S$0.01 to S$0.02.

7 Mr Chua provided two datasets that he claimed to have purchased from Amicus after the Appointed Day. The information disclosed in these datasets are set out in the table below:

	Information Disclosed	**Number of records in the List**
List 1	• partial NRIC number, i.e. the first 4 digits (for some entries); • partial date of birth (for those that did not include a partial NRIC number);[1]	11,384

[1]Amicus admitted that the information it sold to Mr Chua included partial NRIC numbers (i.e. the first 4 digits) but denied that the information contained the individuals' date of birth.

	• gender; and • mobile phone number	
List 2	• partial NRIC number, i.e. the first 4 digits (for some entries); • partial date of birth; • gender; and • mobile phone number	10,074

8 Telemarketers engaged by Mr Chua and his team relied on the information in these datasets to help generate leads and sales for the team by making cold calls to the individuals in the datasets. Mr Chua informed the Commission that Amicus had sold both Lists 1 and 2 to him and confirmed that he did not purchase such lists from any other source at the time. While Amicus admitted that it sold Mr Chua two datasets, it disputed Mr Chua's account that both Lists 1 and 2 were sold to him after the Appointed Day. By Amicus' account, it only sold Mr Chua one dataset after the Appointed Day though it was unable to identify which of the two lists (i.e. Lists 1 and 2) it had sold to Mr Chua.

9 Amicus also admitted to selling the following dataset to another individual on another occasion after the Appointed Day at S$0.10 per record in the course of the investigations:

	Information Disclosed	**Number of records in the List**
List 3	• age; • gender; and • mobile phone number	1,200

10 However, Amicus denied any wrongdoing in selling the datasets with the type of personal data found in Lists 1, 2 and 3 (the "**datasets**") as it contended that the information in the datasets was not personal data to begin with. It also argued that the information in the datasets was publicly available data that it collected from public sources such as Government Gazettes and records of the Singapore Land Authority ("**SLA**") and the Accounting and Corporate Regulatory Authority ("**ACRA**"), and the information in the datasets was collected before the Data Protection Provisions came into effect on the Appointed Day.

11 During investigations, Amicus was unable to give a satisfactory explanation regarding the source of the information in the datasets. Investigations were not able to establish with any degree of certainty when the lists were compiled or obtained, nor where the lists were sourced from [Redacted] (Replaced with Mr L), who is in charge of the day-to-day operations of Amicus, gave evidence on behalf of Amicus and initially claimed that the personal data was obtained from publicly available sources. However, he subsequently claimed that the personal data was obtained from organisers of surveys, meetings and seminars as well as call centres but was unable to name any of the seminars or meetings from which Amicus had purportedly collected the information or the organisations that conducted the surveys or operated the call centres when queried. Thereafter, he claimed that the personal data was obtained from telemarketing and Multi-Level Marketing ("**MLM**") companies, though he was again unable to name any of these companies, nor provide any proof of purchase. Finally, upon further questioning, Amicus represented that the information in the datasets was actually collected before the Appointed Day. He confirmed that he did not collect personal data found in the datasets from publicly available sources.

Number of datasets sold

12 As a preliminary issue, while Amicus and Mr Chua disagreed over the number of datasets that Amicus sold Mr Chua after the Appointed Day[2], an evaluation of the evidence in its entirety shows Mr Chua's evidence to be more credible for the following reasons:

(a) Mr Chua offered the two lists that he claimed to have purchased from Amicus after the Appointed Day even though it was to his detriment. The Commission had commenced investigations on the basis of information provided by a complainant who had requested for anonymity. At the time Mr Chua volunteered the two lists, he was only aware that a complaint had been made against him but was not aware of the information which was provided to the Commission. Hence, the fact that he volunteered information that he knew could be detrimental to himself spoke to his openness and willingness to cooperate with investigations;

(b) although both lists were not dated and he was unable to produce any receipts, Mr Chua was able to produce a screenshot of an email dated 22 March 2016 containing List 1 from one [Redacted] (Replaced with Mr N) from Amicus;

(c) both Lists 1 and 2 only contain partial NRIC numbers, partial date of births, gender and mobile phone numbers. They did not contain names of the individuals. The evidence is that Amicus only started selling lists without names after the PDPA came into

[2] See paragraph 8 above.

effect. Before the PDPA came into effect they sold lists with full names and these lists were more valuable than those sold after the PDPA came into effect. Given that Lists 1 and 2 do not contain full names, it is more likely than not that both these lists were sold after the PDPA came into effect; and

(d) Mr Chua was very cooperative throughout the investigation and there was no evidence to suggest that he had been anything less than forthcoming.

13 In contrast, as described in paragraph 11 above, Amicus had prevaricated during investigations and was unable to give a satisfactory explanation regarding the source of the information in the datasets and was unable to provide any documentary evidence on the dates Lists 1 and 2 were sold. Further, Amicus appeared to have intentionally limited the documentary trail in respect of the sale of Lists 1 and 2. According to Mr Chua, despite allowing its clients, including Mr Chua, to pay for its DNC scrubbing services by cheque, Amicus required cash payment for the lists. Amicus confirmed that it required Mr Chua to pay cash. It is suspicious that a company that has two commercial transactions with the same customer will allow payment for one by cheque but require payment by cash for the other. This conduct is less than straightforward. The reason provided by Amicus for requiring cash payment was that Amicus needed Mr Chua to verify the data in person. The reason provided does not in any way explain why Amicus could not accept cheque payments from Mr Chua when he collected the lists in person.

14 For the foregoing reasons, the following assessment is based on Mr Chua's evidence that Amicus had sold him two datasets (i.e. Lists 1 and 2) after the Appointed Day.

Findings and Basis for Determination

15 The issues for determination are:

(a) whether the information disclosed in the Lists constituted personal data;

(b) whether Amicus had collected, used and/or disclosed personal data without consent and/or notification; and

(c) whether Mr Chua used and/or disclosed the personal data without consent and/or notification.

Whether the information disclosed constituted personal data

16 Section 2(1) of the PDPA defines "personal data" to be data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access.

17 The information disclosed in all three datasets are as follows:

	Information Disclosed	**Number of entries in the List**
List 1	• partial NRIC number, i.e. the first 4 digits (for some entries);	11,384

	• partial date of birth (for those that did not include a partial NRIC number);[3] • gender; and • mobile phone number	
List 2	• partial NRIC number, i.e. the first 4 digits (for some entries); • partial date of birth; • gender; and • mobile phone number	10,074
List 3	• age; • gender; and • mobile phone number	1,200

18 As mentioned at paragraphs 11 and 12 above, although Amicus admitted that it sold datasets containing individuals' mobile phone numbers, age range and gender, it contended that no personal data was disclosed in the datasets because it was "sufficiently anonymised". The datasets did not disclose the individual's name, NRIC number, address or any unique personal information but only included truncated NRIC numbers (i.e. only the first 4 digits) and dates of birth (i.e. only the month and year of birth).

19 There are certain types of information that are unique identifiers, which are capable of identifying an individual in and of themselves. The Advisory Guidelines on Key Concepts in the PDPA sets out a non-exhaustive list of information that the Commission generally considers to be unique identifiers (at [5.10]):

[3]Amicus admitted that the information it sold to Mr Chua included partial NRIC numbers (i.e. the first 4 digits) but denied that the information contained the individuals' date of birth.

(a) Full name;

(b) NRIC number or FIN (foreign identification number);

(c) Passport number;

(d) *Personal mobile telephone number*;

(e) Facial image of an individual (e.g. in a photograph or video recording);

(f) Voice of an individual (e.g. in a voice recording);

(g) Fingerprint;

(h) Iris image; and

(i) DNA profile.

20 In *Re My Digital Lock Pte Ltd* [2018] SGPDPC 3 (at [11]), the Commission observed that information will generally only be considered to be a unique identifier if there is a one-to-one relationship between the information and the individual, i.e. the information is not typically associated with more than one individual:

> **There are certain types of information that in and of themselves are capable of identifying an individual.** The Advisory Guidelines on Key Concepts in the PDPA (revised on 27 July 2017) ("Key Concepts Guidelines") at [5.10] provides a list of information that is considered to be capable of doing so. **While such information is capable of identifying an individual, it does not necessarily mean that anyone in possession of the information will be able to do so**. **The touchstone used to compile the list is the one-to-one relationship of the information and the individual**.

> **Information on the list is not typically associated with more than one individual, either** scientifically (eg biometric signature and DNA profile), by convention (eg NRIC number) or **as a matter of social norms (eg personal mobile phone number)**.
>
> [Emphasis added.]

21 The lists were sold for the purpose of generating leads for the sale of Eldershield and other personal insurance policies. A natural inference is that the mobile numbers in the lists were *personal* mobile numbers. As a personal mobile phone number is generally tied to an individual subscriber who uses it as his/her individual contact number to the exclusion of others, it is *prima facie* personal data given its one-to-one relationship.

22 The "redacted" or truncated NRIC numbers in the datasets do not conform to the Commission's published advisory guidelines on redaction of NRIC numbers which are designed to minimise the risk of re-identification. On the contrary, the key piece of information that the "redacted" NRIC number was intended to convey was the age of the person that it is associated with given that it is well known that the first 4 digits of the NRIC discloses the year of registration (and accordingly, the age) of the individual. It is trite that NRIC numbers are the same as Birth Certificate numbers that are assigned upon registration of birth, which has to take place within x days/weeks of birth. Hence, there was every intention to convey information about the year of birth of the individual associated with the personal mobile phone number.

23 Accordingly, although the information disclosed in the datasets did not include the names of the individuals, the information is still personal data as defined in section 2(1) of the PDPA because the individuals in List 1 and 2 were identifiable directly or indirectly through their year of birth and personal mobile numbers.

24 Likewise, the individuals in List 3 were directly identifiable through their personal mobile phone numbers.

Whether the Organisations breached section 13 and/or section 20 of the PDPA

25 As the PDPA defines "organisation" to include "any individual, company, association or body of persons, corporate or unincorporated", each of Mr Chua and Amicus is an organisation under the PDPA. As mentioned in *Re Spring College International* [2018] SGPDPC 15 (at [10]), the PDPA adopts a consent-first regime and the concepts of notification of purpose and consent are closely intertwined. Pursuant to section 13 of the PDPA, unless an exception to consent is applicable, organisations are generally required to obtain the consent of an individual before collecting, using and/or disclosing the individual's personal data ("**Consent Obligation**"). Consent must be obtained from the individual with reference to the intended purpose of the collection, use or disclosure of the personal data. The organisation's collection, use and disclosure of personal data are limited to the purposes for which notification has been made to the individuals concerned. In this regard, organisations have an obligation under section 20 of the PDPA to inform individuals of the purposes for which their personal data will be collected, used and/or disclosed, on or before collecting the personal data in order to obtain consent ("**Notification Obligation**").

26 As observed in *Re Sharon Assya Qadriyah Tang* [2018] SGPDPC 1 (at [13]), the buying and selling of leads that comprise personal data of individuals are activities that fall under the scope of the PDPA:

> The PDPA governs the collection, use and disclosure of personal data by organisations. Given that the leads which the Respondent had purchased or sold comprised of personal data of individuals,

> these were activities that fell under the scope of the PDPA. **In respect of the purchase of leads by the Respondent, in which the Respondent *acquired* personal data from the seller of the transaction, this amounted to a "collection" of personal data under the PDPA by the Respondent**. **In respect of the sale of leads by the Respondent, in which the Respondent *provided* personal data to the buyer of the transaction, this amounted to a "disclosure" of personal data under the PDPA by the Respondent**.
>
> [Emphasis added.]

Amicus

27 As the organisation with possession and control in respect of the personal data in the datasets that it compiled and sold, Amicus has a duty to comply with the data protection obligations under the PDPA, specifically the Consent and Notification Obligations. However, Amicus contended that it was not necessary for it to obtain consent or to notify individuals before selling the datasets because, among other things[4]:

(a) the information was collected before the Consent and Notification Obligations came into force; or

(b) the information was publicly available.

28 As stated above, Amicus had been prevaricating during investigations without providing a clear and consistent explanation as to when and how the personal data in the Lists were obtained, nor their source. Taking its case at the

[4]Amicus also argued that it was not required to obtain consent and notify the individuals before selling the datasets because the information contained in the datasets are not personal data. We refer to our findings on this issue at paragraphs [18] to [24] above.

highest, the following analysis takes each of these possible defences separately as each, if successful, can stand independently.

Personal data collected before the Appointed Day

29 One of Amicus' main defences was that the information in the datasets was collected before the Data Protection Provisions came into force and Amicus was therefore not subject to the Consent and Notification Obligations in relation to the personal data that it collected, used and/or disclosed. Section 19 of the PDPA allows organisations to continue to use personal data collected before the Appointed Day for the *same purposes* for which the personal data was collected without obtaining fresh consent, unless consent for such use is withdrawn. As such, it may be possible for an organisation to continue using personal data that was purchased or obtained before the Appointed Day without consent or notification if such use falls within the purposes of collection, provided that there was no indication that the individual did not consent to the continued use[5].

30 However, section 19 of the PDPA only covers the *use* of personal data collected before the Appointed Day and not the *disclosure* of personal data. As was held in *Re Sharon Assya Qadriyah Tang* (at [22] and [23]), the grandfathering provision in section 19 of the PDPA would not apply to instances where the organisation had been selling personal data before the Appointed Day, and continued to sell personal data after the Appointed Day:

> However, in this case, the Respondent went beyond using the personal data for her own telemarketing purposes, and proceeded to sell personal data to third parties. The "grandfathering" provision only permits the continued "use" of personal data for

[5] *Re Sharon Assya Qadriyah Tang* (at [20])

> the purposes for which the personal data was collected. Such "use" does not extend to "disclosure" of personal data unless, as set out at paragraph 23.1 of the Advisory Guidelines, the disclosure "is necessarily part of the organisation's use of such personal data". **In the case of the sale of personal data, the disclosure of personal data is the main activity being carried out, and is not incidental to any of the organisation's own uses of the personal data. Thus, it is not a disclosure "that is necessarily part of the organisation's use of such personal data".** The Commission has stated this position in its Advisory Guidelines as an example:
>
> > Organisation XYZ has been selling databases containing personal data. This would be considered a disclosure of personal data and not a reasonable existing use under section 19. After the appointed day, XYZ needs to ensure that consent has been obtained before selling these databases again.
> >
> > [Emphasis added.]
>
> **Consequently, the grandfathering provision would not apply to the instances where the Respondent had been selling personal data before the Appointed Day, and continued to sell personal data after the Appointed Day.** In respect of personal data that was not sold before the Appointed Day, it is all the more so that the Respondent cannot rely on the grandfathering provision, because there was never an existing practice of selling the personal data in the first place, and hence there is no "use" to be carried on in respect of the personal data.
>
> [Emphasis added.]

31 Moreover, even if Amicus had collected the personal data before 2 July 2014, that permitted it to disclose by way of sale, it would have had to obtain fresh consent for such purposes of disclosure after the Appointed Date. Needless to say, Amicus was not able to provide evidence of either during the course of investigations. As mentioned at paragraph 11 above, Amicus was unable to satisfactorily explain the source of the personal data in the datasets. During the

course of the investigation, Amicus first claimed that the information was collected from surveys, meetings and seminars, but subsequently represented that it was collected from telemarketing and MLM companies. Nevertheless, even if the individuals had provided their personal data during surveys or at meetings and seminars, or even if the personal data was collected from telemarketing or MLM companies, Amicus did not provide any evidence that the individuals concerned had provided fresh consent after the Appointed Date for their personal data to be disclosed by way of sale to telemarketers. In this regard, Amicus acknowledged that it could have sought consent given that it possessed the individuals' full NRIC numbers and personal mobile phone numbers but conceded that it did not do so.

32 In the circumstances, there was a clear breach of the Consent and Notification Obligations under the PDPA in respect of Amicus' sale of the datasets containing personal data after the Appointed Day.

Publicly available exception

33 The alternate defence that Amicus raised during the investigations, but which it subsequently dropped, was that the information in the datasets was publicly available information obtained from public sources, such as records of registered doctors, lawyers and engineers published on Government Gazettes, and records from SLA and ACRA. The PDPA sets out an exception for the collection, use and disclosure of personal data that is publicly available.[6] However, by Amicus' own admission, the Government Gazettes only contained

[6]Paragraph 1(c) of the Second Schedule to the PDPA; paragraph 1(c) of the Third Schedule to the PDPA; and paragraph 1(d) of the Fourth Schedule to the PDPA.

the names and organisations of certain individuals, which did not form part of the information that was found in the datasets it sold after the Appointed Day.

Representations by Amicus and an affiliated company

34 Amicus and an affiliated company, Ilied.com Pte. Ltd. ("**Ilied**"), submitted written representations to the Commission (the "**Representations**") after Amicus received a copy of the Preliminary Decision. The Representations were signed off by Mr L. In the Representations, Ilied and Amicus raised the following three points:

(a) Ilied was the organisation that sold the datasets, and not Amicus;

(b) List 1 was transacted before the Appointed Day; and

(c) The datasets did not contain personal data as they had been truncated and anonymised, and further, that personal mobile phone numbers are not personal data *per se*.

The identity of the organisation which sold the datasets

35 The Representations enclosed two invoices issued by Ilied in support of the assertion that it was Ilied which had sold the data (the "**Invoices**"). The first Invoice, for the sum of $1,900, was dated 25 June 2014 and was issued for "Leads Born 1973, 1975". The second Invoice, for the sum of $1,138, was dated 22 March 2016 and was issued for "Data Sales".

36 Ilied is an affiliate of Amicus and together with Amequity Solutions Pte Ltd ("**Amequity**"), are part of a group of closely related companies managed by Mr L, with some of the shareholders and directors being common across the said affiliated companies.

37 The Commission has reviewed the Representations and the additional evidence and finds that on a balance of probabilities, Amicus sold the data.

38 Ilied attempted to use the Invoices as incontrovertible proof that it was Ilied, and not Amicus, which had sold the datasets. However, Mr L, Mr N and [Redacted] (Replaced with Ms J), the Director and shareholder of Amicus, Ilied and other affiliated companies, stated in their statements to the Commission that Amicus, Ilied and all affiliated companies operated as a single entity, with no clear demarcation between the companies. The entire group of companies was, in effect, headed by Mr L. Ilied individually had no real function but was merely used "for receipt purpose"[7] and it did not even have a bank account.[8] The facts suggest that Ilied's issuance of the Invoices was merely an administrative arrangement and that Ilied, in fact, did not engage in data sales.

39 Furthermore, Amicus' vacillation in its responses to the Commission also suggests that Amicus' new claim that Ilied was the data seller should be treated with circumspection. As noted at paragraph 52(d) below, Amicus was inconsistent in its responses and kept changing its account of the facts. In particular, Amicus provided inconsistent accounts on the source of the personal data, initially claiming that it was collected from publicly available sources, subsequently claiming that it was collected from surveys, meetings and seminars, and finally claiming that it was collected from telemarketing and MLM companies. Amicus was also inconsistent in its statements concerning Amequity. Amicus stated in the Representations that Amequity "is not into data business, but credit collection by banks". However, in the same

[7] Mr N's statement dated 30 April 2019.

[8] Mr L's statement dated 30 April 2019.

Representations, Amicus also stated that one of the lists of personal data, dated 5 March 2014, had been sold by Amequity.

40 Amicus, through its representatives Mr N and Mr L, admitted initially that it was Amicus that sold the datasets. This was corroborated by Mr Chua. Mr N explained Ilied's issuance of the receipt by stating that Ilied, like Amequity, had no real function but was used for "receipt purpose". Mr L also admitted in his statement given on 3 February 2017 that "data selling is purely done by Amicus". There is no reason to distrust the consistent evidence of all three individuals, reflected in separate statements recorded at different times.

41 Amicus subsequently tried to explain this away by saying that Mr L's statement referred to above at paragraph 40 were made "with reference to the business done by Amicus vis-à-vis Amequity", and that "the term Amicus was used loosely to refer to company that do data sales [sic]". Amicus further claimed that it had "confused itself" to be the seller because the Commission's Notice to Require Production of Documents and Information ("**NTP**") was addressed to it. If it was true that both Amicus and Ilied engaged in data selling, this would have been operative on Mr L's mind when answering the NTP and at the very least raised the possibility that it may have been Ilied which sold the data instead, earlier in the investigations. The fact that all three individuals, Mr N, Mr L and Mr Chua, were consistent in omitting to mention Ilied during the investigations shows that it was only Amicus that was engaged in data sales. The reasonable explanation is that while the invoices may have been issued by other companies affiliated to Amicus, such as Ilied or Amequity, it was Amicus that in fact engaged in data sales and Ilied and Amequity's part in the arrangement was to merely issue invoices.

42 For the above reasons, it is more likely than not that Amicus sold the data to Mr Chua. Accordingly, the assertion in the Representations that it was Ilied which had sold the data cannot be accepted.

Date of transaction for List 1

43 Ilied claimed that the first Invoice was a receipt for List 1, and as the first Invoice was dated 25 June 2014, List 1 was transacted before the Appointed Day. However, it is unlikely that the first Invoice was a receipt for List 1. The quantity reflected on the first Invoice is 19,000, whereas the quantity of records in List 1 was 11,384. On the facts, it is more likely that List 1 was transacted on 22 March 2016, i.e. after the Appointed Day, for the following reasons:

(a) As noted at paragraph 12(b) above, Mr Chua was able to produce a screenshot of an email from Mr N, containing List 1. The email was dated 22 March 2016, which was the same as the date on the second Invoice;

(b) The second Invoice, which was dated 22 March 2016, was more likely to be the receipt for List 1;

(c) Mr N corroborated in his statement that List 1 was sold on 22 March 2016;

(d) List 1 contained personal data of individuals born in 1976 whereas the first Invoice was issued for "Leads Born 1973, 1975";

(e) The second Invoice reflected a quantity of 11,380, which was closer to the quantity of records in List 1 than the quantity reflected in the first Invoice; and

(f) As noted at paragraph 18 above, List 1 contained truncated personal data. As noted in paragraph 45 below, the truncation had apparently been done in an attempt to comply with the requirements of the PDPA and, as such, List 1 was more likely to have been transacted after the Appointed Day.

44 In view of the above factors, the weight of the evidence points to the fact that List 1 was transacted after the Appointed Day.

Whether the datasets contained personal data

45 In the Representations, Ilied claimed that it sought to comply with the requirements of the PDPA by truncating and anonymising the personal data. As noted at paragraph 22 above, the "redacted" or truncated NRIC numbers in the datasets do not conform to the Commission's published advisory guidelines on redaction of NRIC numbers. The "redacted" NRIC numbers were intended to, and did in fact, convey information about the year of birth of the individual associated with the personal mobile phone number.

46 Ilied further claimed in the Representations that its research showed that an individual's mobile phone number is *likely* to be personal data as it *may* be uniquely associated with an individual, but stopped short of admitting that all mobile phone numbers were personal data. In this regard, Ilied has not raised any evidence or arguments to suggest that the personal mobile phone numbers disclosed in the datasets were not personal data. As stated at paragraphs 19 to 21 above, personal mobile numbers are *prima facie* personal data as they are unique identifiers.

Mr Ivan Chua

47 As observed in *Re Sharon Assya Qadriyah Tang* (at [13]), the purchase of leads, in which the buyer acquired personal data from the seller of the transaction amounts to a "collection" of personal data under the PDPA by the buyer. It is not disputed that Mr Chua collected personal data when he bought the Lists from Amicus and used the personal data to market his team's financial products. By his own admission, the personal data was collected and used in breach of the Consent and Notification Obligations. Mr Chua also admitted that while he received verbal assurance from Amicus that the information in the datasets was obtained from caveats and was "legal", he did not probe further as to how, where and when Amicus obtained the personal data, or whether Amicus had obtained consent and provided notification to the individuals concerned.

48 In this regard, reference is made to the UK Information Commissioner's Office's ("**ICO**") decision in *The Data Supply Company*, where a data broker was found to be in breach of the Data Protection Act 1998 for obtaining customer data from various sources and selling the data to third party organisations for the purposes of direct marketing. The individuals were not informed that their personal data would be disclosed to the data broker, or the organisations to which the data broker sold the data on to, for the purpose of sending direct marketing text messages. The ICO issued a monetary penalty of £20,000 and gave the following guidance in the Monetary Penalty Notice (at [22] to [25]):

> **Data controllers buying marketing lists from third parties must make rigorous checks to satisfy themselves that the third party obtained the personal data fairly and lawfully, that the individuals understood their details would be passed on for marketing purposes, and that they have the necessary consent.**
>
> Data controllers must take extra care if buying or selling a list that is to be used to send marketing texts, emails or automated calls.

The Privacy and Electronic Communications Regulations 20003 specifically require that the recipient of such communications has notified the sender that they consent to receive direct marketing messages from them. Indirect consent (ie consent originally given to another organisation) may be valid if that organisation sending the marketing message was specifically named. But more generic consent (eg marketing 'from selected third parties') will not demonstrate valid consent to marketing calls, texts or emails.

Data controllers buying in lists must check how and when consent was obtained, by whom, and what the customer was told. It is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence. Such due diligence might, for example, include checking the following:

- How and when was consent obtained?
- Who obtained it and in what context?
- What method was used – eg was it opt-in or opt-out?
- Was the information provided clear and intelligible? How was it provided – eg behind a link, in a footnote, in a pop-up box, in a clear statement next to the opt-in box?
- Did it specifically mention texts, emails or automated calls?
- Did it list organisations by name, by description, or was the consent for disclosure to any third party?
- Is the seller a member of a professional body or accredited in some way?

Data controllers wanting to sell a marketing list for use in text, email or automated call campaigns must keep clear records showing when and how consent was obtained, by whom, and exactly what the individual was told (including copies of privacy notices), so that it can give proper assurances to buyers. Data controllers must not claim to sell a marketing list with consent for texts, emails or automated calls if it does not have clear records of consent. It is unfair and in breach of the first data protection principle to sell a list without keeping clear records of consent, as it is likely to result in individuals receiving noncompliant marketing.

[Emphasis added.]

49 While there is no uniform industry standard in relation to how a buyer should verify whether the seller has obtained the consent of the individuals, the positions articulated by the ICO must be right. A reasonable person would likely undertake proper due diligence, such as seeking written confirmation that the personal data sold was actually obtained via legal sources or means, or inquire further as to whether the individuals had provided their consent and were notified of the disclosure, and if so, obtain a sample of such consent and notification.

50 Similarly, organisations that sell datasets should ensure that they obtain and maintain clear records of consent so that proper assurances can be given to buyers.

Directions

51 Having found Amicus and Mr Chua to be in breach of sections 13 and 20 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to give such directions as he deems fit to ensure compliance with the PDPA.

52 In assessing the breach and determining the directions to be imposed on Amicus, the following aggravating factors were taken into account:

(a) the personal data disclosed included NRIC numbers which constitute personal data of a sensitive nature;

(b) Amicus profiteered from the sale of personal data. It admitted that it sold the personal data to others besides Mr Chua;

(c) Amicus was unhelpful and was not forthcoming in its responses to the Commission during the investigation; and

(d) Amicus was inconsistent in its responses and kept changing its account of the facts.

53 The following aggravating and mitigating factors were taken into account in assessing the breach and determining the directions to be imposed on Mr Chua:

Aggravating factors

(a) the personal data was purchased with the intention to market goods and services to individuals for financial gain; and

Mitigating factors

(b) Mr Chua had cooperated fully with the investigation and played an important and integral role in the investigation. He was forthcoming and admitted to his wrongdoing at the first instance.

54 There are strong policy reasons for taking a hard stance against the unauthorised sale of personal data, which were set out in *Re Sharon Assya Qadriyah Tang* (at [30]):

> The Commissioner likewise **takes a serious view of such breaches under the PDPA. There are strong policy reasons for taking a hard stance against the unauthorised sale of personal data**. Amongst these policy reasons are **the need to protect the interests of the individual and safeguard against any harm to the individual, such as identity theft or nuisance calls**. Additionally, there is a need to **prevent abuse by organisations in profiting from the sale of the individual's personal data at the individual's expense**. It is indeed such cases of potential misuse or abuse by organisations of the

> individual's personal data which the PDPA seeks to safeguard against. In this regard, the Commissioner is prepared to take such stern action against organisations for the unauthorised sale of personal data.
>
> [Emphasis added.]

55 The profiting from sale of personal data by organisations without consent of individuals is the kind of activity which the PDPA seeks to curb and will be dealt with severely. In order to prevent abuse by organisations profiting from the sale of personal data at the individual's expense, the Commission may take into account any profits from the unauthorised sale of personal data in calculating the appropriate financial penalty to be imposed.

56 Having considered all the relevant factors of this case, the following directions are made:

To Amicus:

(a) to pay a financial penalty of $48,000 (including $2,900 for the profit made from the sale of Lists 1 and 2) within 30 days from the date of the Commissioner's direction, 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;

(b) to cease the disclosure (sale) of the personal data of all the individuals immediately;

(c) to cease the retention of the said personal data within seven (7) days from the date of the Commissioner's direction, to the extent

that such personal data was collected and/or disclosed in breach of the PDPA; and

(d) to submit a written confirmation to the Commission by no later than 1 week after each of the above directions in (b) and (c) have been carried out.

To Mr Ivan Chua:

(e) to pay a financial penalty of $10,000 within 30 days from the date of the Commissioner's direction, 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;

(f) to cease the use (telemarketing) of the personal data of all the individuals immediately;

(g) to cease the retention of the said personal data within seven (7) days from the date of the Commissioner's direction, to the extent that such personal data was collected in breach of the PDPA; and

(h) to submit a written confirmation to the Commission by no later than 1 week after each of the above directions in (f) and (g) have been carried out.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION