Decision of Restricted Committee No. SAN-2021-020 of 28 December 2021 concerning [redacted]

The Commission nationale de l'Informatique et des Libertés (CNIL - French Data Protection Agency), met in its Restricted Committee consisting of [redacted]

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data;

Having regard to the amended French Data Protection Act No. 78-17 of 6 January 1978, in particular Articles 20 *et seq.*;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Decision No. 2013-175 of 4 July 2013 adopting the rules of procedure of CNIL (French Data Protection Agency);

Having regard to Decision No. 2020-107C by the CNIL Chair of 12 May 2020 to instruct the Secretary General to carry out or have carried out an audit of the [redacted]

Having regard to the decision of CNIL's Chair appointing a rapporteur before the Restricted Committee of 12 April 2021;

Having regard to the report of [redacted] commissioner rapporteur, notified to [redacted] on 23 June 2021;

Having regard to the written observations made by [redacted] on 23 July 2021;

Having regard to the oral observations made at the Restricted Committee session;

Having regard to the other documents in the file;

The following were present at the Restricted Committee session on 16 September 2021:

- [redacted], Commissioner, heard in her report;

In the capacity of representatives of [redacted]:

- [redacted]
-
-
-

[redacted] having last spoken;

After having deliberated, the Restricted Committee adopted the following decision:

I. Facts and proceedings

1. [redacted] (hereinafter the "company") is a public limited company, registered with the Paris Trade and Companies Register, whose business is to advise on computer systems and software. It has [redacted] employees.

2. The company is an authorised payment institution, which offers recurring payment services in the "Single Euro Payments Area"– (SEPA). It offers its customers, "merchants" who are legal entities, solutions for managing subscriptions and recurring payments.

3. As part of the services provided by the company to its merchants, the personal data processed is that of the merchants' debtors who are natural persons. As at 1st September 2020, [redacted] had [redacted] debtors who are natural persons from the merchants in its databases.

4. In 2019, it generated turnover of [redacted] and a net loss of [redacted] In 2020, it generated turnover of [redacted] and a net loss of [redacted]. The company also raised [redacted] in 2015.

5. In the summer of 2015, as part of an internal research project on an anti-fraud mechanism, the company re-used personal data contained in its databases for testing purposes. It has thus imported debtors' personal data on a server. When the research project ended in July 2016, the data remained on this server, which was not subject to any special security procedures and was still freely accessible from the Internet.

6. On 14 February 2020, one of the company's merchant customers reported this information to the company. [redacted] then immediately isolated the server and sequestered the data, in order to end the personal data breach.

7. On 17 February 2020, the company notified the data breach to the Commission nationale de l'informatique et des libertés (French Data Protection Agency) (hereinafter referred to as the "Commission" or "CNIL").

8. On 26 February 2020, the company submitted a supplementary data breach notification to CNIL, providing further details on the security incident, including the measures implemented by the company, the number of individuals and the type of personal data affected by the data breach.

9. The debtor data of [redacted] merchants, corresponding to approximately twelve million unique debtors, was affected by this breach. The personal data affected by the breach are civil status data (title, last name, first name), postal, e-mail and telephone details, and bank details ("*Bank Identifier Code*" - BIC/ "*International Bank Account Number*" - IBAN).

10. As the information provided helped to establish the cross-border nature of the processing concerned, CNIL informed all the European supervisory authorities on 27 February 2020, in accordance with Article 56 GDPR, of its competence to act as lead supervisory authority, and thus opened the procedure for the declaration of the authorities concerned in this case.

11. Pursuant to Decision No. 2020-107C of the Chair of the Commission of 12 May 2020, CNIL carried out a documentary investigation with the company to verify its compliance with all the provisions of the amended French Data Protection Act No. 78-17 of 6 January 1978 and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the "GDPR"). This task was carried out by sending a questionnaire, sent by registered letter with acknowledgement of receipt on 31 July 2020.

12. In an email dated 5 August 2020, the company's Data Protection Officer requested additional time from the CNIL delegation.

13. In an email dated 6 August 2020, the company was granted an extension until 11 September 2020.

14. On 11 September 2020, the company sent elements of its response to CNIL, by secure electronic means.

15. By emails dated 21 October and 2 December 2020, the CNIL delegation requested additional information from the company, in particular in order to find out whether the company had made a public announcement or taken any other similar action to inform the data subjects of the data breach and whether the research and development work it was doing as part of the fight against fraud required the use of non-anonymised real data. These elements were submitted respectively on 29 October and 10 December 2020.

16. In order to examine this case, the CNIL Chair appointed [redacted] as rapporteur on 12 April 2021, pursuant to Article 39 of Decree No. 2019-536 of 29 May 2019 implementing the amended French Data Protection Act of 6 January 1978.

17. At the end of her investigation, on 23 June 2021, the rapporteur notified [redacted] of a report detailing the breaches of the GDPR that she considered demonstrated in this case. It was also given a letter informing it that the case file was on the agenda of the Restricted Committee of 16 September 2021.

18. This report proposed to the Restricted Committee of the Commission to impose an administrative fine against the company, in view of the demonstrated breaches of Articles 28 (3) and (4), 32, and 34 GDPR. It also proposed that the sanction decision be made public and that the company no longer be identifiable by name upon expiry of a period of two years following its publication.

19. On 23 July 2021, the company submitted observations in response.

20. The company and the rapporteur presented oral observations at the meeting on 16 September 2021.

II. Reasons for the decision

21. According to Article 56(1) of the Regulation "*the supervisory authority of the main establishment or sole establishment of the controller or processor shall be competent to act as lead supervisory authority regarding the cross-border processing operation carried out by that controller or processor, in accordance with the procedure laid down in Article 60*".

22. In this case, the Restricted Committee notes that the registered office of the company, the sole establishment of [redacted], is located in France and has been registered with the Trade and Companies Register in France since the start, which leads CNIL to become the competent supervisory authority concerning the cross-border processing carried out by this company, in accordance with Article 56 (1) of the Regulation.

23. In accordance with the cooperation and coherence mechanism provided for in Chapter VII of the GDPR, on 27 February 2020 CNIL informed all European supervisory authorities of its competence to act as the lead supervisory authority concerning the cross-border processing carried out by the company and opening the Notification procedure for the relevant authorities in this case. The supervisory authorities of the following countries declared themselves concerned in this procedure: Germany, Spain, Italy and the Netherlands.

24. On 25 November 2021, the draft decision adopted by the restricted committee was submitted to these supervisory authorities, in accordance with Article 60 (3) of the GDPR.

25. On 24 December 2021, none of the supervisory authorities concerned had raised any relevant and reasoned objections to the draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

A. <u>On the status of the company in terms of processing liability</u>

26. Under Article 4 GDPR, the controller is defined as "*the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing " (point 7) and the processor is "* (point 7) and the processor is "*the natural or legal person, the public authority, agency or other body which processes personal data on behalf of the controller*" (point 8).

27. Article 28-10 GDPR provides that "*without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing*."

28. The rapporteur notes that [redacted] acts as data controller concerned by the data breach and as a processor for the processing carried out in the context of the services provided to merchants, data controllers.

29. In its defence, the company does not dispute the rapporteur's analysis on this point.

30. The Restricted Committee considers that the notion of controller must be assessed in a practical way, taking into account all the elements that make it possible to attribute this status to an entity. In this respect, it notes that it is clear from the information provided to CNIL that [redacted] acts as data processor for the processing carried out in the context of the services provided to merchants, data controllers, insofar as the company does not determine the purposes of data processing. These services are the main part of its business (recurrent payment services, SEPA mandates, etc.).

31. The Restricted Committee also notes that the company itself uses, as part of the services provided to merchants, the services of data processors. As the company states, [redacted]'s processors are therefore sub-processors to the merchants.

32. The Restricted Committee also considers that [redacted] acted as the data controller concerned by the data breach, this being internal research processing concerning a mechanism to combat fraud, whose purposes and means it alone determined. The company itself states that it is acting as a data controller in the additional data breach notification it sent to CNIL on 26 February 2020.

33. It is therefore up to the Restricted Committee to examine, in the light of these qualities, the objections raised by the rapporteur against the company.

B. <u>On the characterisation of breaches with regard to the GDPR</u>

34. First of all, the Restricted Committee notes that, in its defence, the company contests the fact that breaches unrelated to the personal data breach may be retained, while that is at the origin of the proceedings.

35. The Restricted Committee considers that the fact that CNIL's investigations were initially motivated by the occurrence of the data breach, following its notification, has no impact on the possibility of finding the existence of other breaches of the GDPR in view of the facts found in the investigations carried out by the CNIL's monitoring delegation.

36. Indeed, it is clear from Article 8 of the French Data Protection Act that CNIL, on the one hand, may carry out checks on all processing operations and, where applicable, obtain copies of all documents or information media useful for its tasks, on the other hand, it must ensure that the processing of personal data is carried out in accordance with the provisions of said Act and other provisions relating to the protection of personal data provided for by the legislative and regulatory texts, European Union law and France's international commitments.

37. In this context, and under Article 20 of the "French Data Protection Act", the Restricted Committee shall take measures and impose sanctions against data controllers or data processors who do not comply with the obligations arising from the GDPR and said Act.

<u>1. On the failure to provide a formal legal framework for the processing operations carried out by a sub-processor</u>

38. Under Article 28(3) GDPR, "*Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:*

> *a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*
>
> *b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*
>
> *c) takes all measures required pursuant to Article 32;*

d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; [...]".

39. Pursuant to paragraph 4 of the same Article, where a processor engages another processor to carry out specific processing activities on behalf of the controller, the same data protection obligations as those set out in the contract between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act, in particular as regards the provision of sufficient guarantees to implement appropriate technical and organisational measures so that the processing operation complies with the Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of the other processor's obligations.

40. During the investigations conducted by CNIL, [redacted] indicated that it uses processors acting under its authority as sub-processors for merchants, for services that it provides to the latter (recurring payment services, SEPA mandates, etc.) The company also said that it sends the processors a "*questionnaire relating to processing*" in order to comply with the GDPR. The questionnaire states: "*in its capacity as a payment service provider,* [redacted] *is committed to complying with the provisions of the General Personal Data Protection Regulation (Regulation (EU) 2016/679). To this end, we must ensure that the data processing carried out by our partners complies with legal requirements*".

41. The rapporteur considered that the steps taken by the company to its data processors through these questionnaires were not sufficient to meet its obligations and to ensure that the sub-processors provide sufficient guarantees. It also noted that the contracts and amendments entered into with three companies did not contain all the clauses provided for by Article 28 (3) GDPR and that those concluded with three other companies did not contain any of the mandatory information provided for by the same article.

42. In its defence, the company explains that it is implementing concrete measures to ensure its compliance with data protection regulations as part of an ongoing approach, not only by relying on the compliance documentation provided by its subcontractors, which propose standard contractual commitments, but also through one-off questionnaires. It specifies that the purpose of the questionnaires sent during CNIL's control was to justify checks carried out by [redacted] with its data processors, adding that, in the absence of the said data processors providing contractual documentation governing data protection guarantees, it is planned to subject them to such an agreement. [redacted] also reports on ongoing negotiations with certain companies on the signing of amendments relating to the protection of personal data.

43. **Firstly**, the Restricted Committee notes that the company has not provided evidence that this questionnaire is filled out by sub-processors. In any event, even if it were, the Restricted Committee stresses that the questionnaire is only declaratory and does not constitute a binding legal act by which the sub-processor undertakes to comply with the elements defined. The sending of this questionnaire does not therefore meet the obligations laid down in Article 28(3) and (4).

44. **Secondly**, the Restricted Committee notes that some of the contracts concluded by the company with its processors do not contain all the clauses provided for in Article 28(3) GDPR: In this sense, it notes that the contracts and amendments concluded with the group [redacted] and its subsidiary [redacted], concerning the presentation and receipt of SEPA flows to European interbank exchange systems, do not specify all the

information required under Article 28 GDPR, in particular the type of data concerned and the obligations and rights of the Data controller; Likewise, in the contract and amendments concluded with [redacted], concerning the provision of an advanced digital signature solution, the type of data and the obligations and rights of the Data controller are not mentioned.

45. The Restricted Committee also notes that the contracts and amendments entered into with [redacted] (concerning the service for sending one-time password (OTP) codes allowing an advanced electronic signature), [redacted] (concerning data hosting for a particular merchant) and [redacted] (concerning data hosting) do not contain any of the mandatory information provided by Article 28 GDPR.

46. **Thirdly**, the Restricted Committee notes that [redacted] provided, within the framework of the sanction procedure, an example of a "personal data protection" amendment concluded with [redacted] in July 2021 and that it specified that negotiations are in progress with the companies [redacted], [redacted], and [redacted] The Restricted Committee takes note of partial compliance under this procedure. Nevertheless, the fact that the company had taken steps with the data processors in the context of this procedure clearly demonstrates that it was not in compliance at the time of the investigations carried out by CNIL.

47. Moreover, it is still not in compliance with regard to certain contracts, thus continuing to disregard the obligation to regulate by a formalised legal act the processing carried out by a sub-processor.

48. Therefore, with regard to all of these elements, the Restricted Committee considers that the breach of Article 28 (3) and (4) GDPR is established.

2. On the breach of the obligation to ensure the security of personal data

49. Under Article 32 GDPR: *"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed […]".

a) On the security failure that led to the personal data breach

- *Characterisation of the breach*

50. The rapporteur notes that it is clear from the information provided to CNIL that, as part of a research project carried out in 2015, [redacted] re-used debtors' personal data for the purpose of testing a mechanism to combat fraud. The project ended the following year, in July 2016, but the data remained on a server with no special security measures. On 14 February 2020, the company was notified by one of its customers of the possibility of freely accessing this data from the Internet by means of a URL consisting simply of an IP address and a communication port, without any other access restrictions or security measures. That same evening, the company isolated the server containing the personal data concerned.

51. According to the rapporteur, the breach committed by the company with regard to its security obligation thus started in 2015, when the data of merchants' customers were imported on a server not subject to any security measure, and it lasted, since it only ended in February 2020, after the company was alerted by one of its customers. She considers, given that this is a continuous breach, that it should be sanctioned from the point of view of the GDPR and that such an analysis was recently supported by the French Conseil d'Etat in its decision of 1st March 2021 concerning *Futura Internationale*.

52. With regard to the facts establishing non-compliance, the rapporteur points out that access to the server in question was not subject to any satisfactory access restriction measures and that the company had not put in place any measure to log access to the server.

53. In its defence, [redacted] disputes the analysis of the rapporteur in which the principle of non-retroactivity of the more severe criminal penalty cannot be applied to breaches that continue to produce effects over time, to the extent that even if they began under the French Data Protection Act, they persist under the GDPR and must therefore be qualified as continuous and understood, for the period following the entry into force of the GDPR, by the application of the provisions of said Regulation. To this end, it also relies on the judgement of the French Conseil d'Etat of 1st March 2021 on *Futura Internationale*, considering that this case law applies to a special case distinct from this case: in the *Futura Internationale* judgement, the French Conseil d'Etat took care to clarify that deliberate breaches had not been corrected despite CNIL's formal notice. This case law can therefore not be transposed to the present case according to the company insofar as it has automatically been proposed a sanction without formal notice or prior injunction from CNIL and that it also collaborated diligently and in good faith with CNIL as soon as the incident was notified.

54. In addition, [redacted] explains that the vulnerability of the server is the result of isolated human negligence and not a shortcoming of its technical and organisational system. It recalls that the general security obligation of companies must be analysed as a best-efforts obligation and not a performance obligation. It adds that it ended the data breach immediately after being informed of it. It also indicates that the use of data stored on the server required computer knowledge and the use of specific tools, that the data present on the server dated from 2012 to 2013 and that, therefore, it was difficult to exploit by an attacker. Finally, it notes that the IP address of the server was not referenced on any search engine.

55. During the Restricted Committee session, the company stated that the human negligence mentioned in its submissions was in fact attributable to [redacted] It broadly insisted that it had not committed, as a data controller, any breach of its security obligations to the extent that the error was committed by [redacted] to deal with the security of the systems.

56. **Firstly**, with regard to the principle of non-retroactivity, the Restricted Committee considers that, insofar as the personal data breach, as well as the lack of security in which it found its origin, lasted after 25 May 2018, the date of the entry into force of the GDPR, it is in the light of this text that the breaches alleged against [redacted] must be assessed. This analysis was supported by the French Conseil d'Etat in its decision of 1st March 2021 concerning *Futura Internationale*. In that case, following a complaint relating to telephone solicitation by Futura Internationale, the Conseil d'État considered that, if the breaches by the company were found during an investigation carried out by CNIL before the GDPR came into force, they continued after that date. The Conseil d'État concluded that "*it is thus right that CNIL, noting the continuing nature of the breaches noted* […], *considered the GDPR applicable to the facts of the case and assessed the breaches in view thereof"* (French Conseil d'Etat, 10th- 9th chambers, 1March 2021, *Futura Internationale*, No. 437808).

57. The Restricted Committee recalled, first of all, that in accordance with Article 20 of the French Data Protection Act, the CNIL Chair is not required to send a formal notice to the organisation before initiating sanction proceedings against it.

58. **Secondly**, the Restricted Committee notes that access to the server in question was not subject to any satisfactory restriction of access measures, insofar as it was possible to access it from an URL composed of an easily identifiable IP address using port scanning programs, which are available on the web and often used by attackers to detect unsecure or poorly secure servers.

59. The Restricted Committee also notes that the company had not implemented any system to log access to the server, which would have made it possible to detect the actions carried out on the server. Indeed, the establishment of logging of activities, that is to say, recording activities in "log files" or "logs," particularly for access to the various servers of an information system, is crucial in that it enables the activities to be traced and to detect any anomalies or events related to security, such as fraudulent access and misuse of personal data. Thus, in its security recommendations for the implementation of a logging system, the Agence nationale de la sécurité des systèmes d'information (ANSSI) noted that "*event logs are a technical brick that is essential for the security management of information systems*" to the extent that they can be used "*a priori to detect security incidents*" and *a posteriori* to "*understand the path of an attack and* […] *assess its impact*".

60. The Restricted Committee also notes that the data contained on the server could easily be read as it was stored in legible formats by means of a simple text editor or tools available and well documented on the Internet.

61. Thus, the absence of a security measure protecting the server in question, particularly restricting access only to individuals who should have been authorised, caused the data concerned to be accessible from the Internet and that data was easily readable due to the format in which it was stored.

62. **Thirdly**, the Restricted Committee considers that the company's argument, saying that it would not be liable for the breach of its security obligations insofar as the error was committed by its [redacted], is not convincing.

63. First of all, the Restricted Committee notes that security deficiencies are not the result of an isolated human error, but from repeated insufficiency, since the company should have ensured the security of the data in question at several stages. In this regard, when it decided to reuse the

data for its internal project, it was up to the company to check that the server used for such purposes was only accessible by authorised persons. The same monitoring requirement was at least necessary for the company when it completed its research project. Also, the company cannot reject the liability for such repeated deficiencies on an isolated human error by its [redacted], who, in any event, acted in his capacity as an employee on the instructions of the company and on its behalf.

64. Secondly, the security of an information system is based on a set of technical and procedural measures, and not solely on the competence of individuals, even if it was the [redacted]. The effective implementation of these technical and procedural measures must precisely address human deficiencies. The company should therefore have provided for additional safeguards. The Restricted Committee considers that this situation reflects an organisational problem within the company.

65. Therefore, the Restricted Committee considers that [redacted] breached its obligation resulting from the provisions of Article 32 of the Regulation.

- *Scope of the breach*

66. The company argues that the breach did not cause any harm to the data subjects concerned by the personal data breach, since none of these individuals notified it of the fraudulent use of their personal data. It explains having had an audit carried out by a third party company, [redacted], after the discovery of the vulnerability, which shows that the data present on the server were not exploited by an attacker.

67. With regard to the scope of the breach, the Restricted Committee noted that it is apparent from the notification sent to CNIL on 26 February 2020 that the personal data breach compromised the personal data of 12,478,819 European nationals.

68. The Restricted Committee considers that the lack of evidence of fraudulent use of the data does not affect the characterisation of the breach of the security obligation. Indeed, the risk of fraudulent use of personal data was real, independent of cases of fraud, insofar as the data of many individuals were made available to unauthorised third parties. The absence of proven damage for the data subjects has no impact on the existence of the security deficiency, which constitutes the breach of Article 32 GDPR.

69. The Restricted Committee also recalls that civil status data (title, surname, first name), postal, electronic and telephone contact information, and banking information (BIC/IBAN) were compromised.

70. It points out in this respect that, in view of the nature of such personal data, the data subjects concerned by the breach are exposed to the risk of re-use of their personal data by attackers. Indeed, they face the risk that their directly identifying data will be the subject of unlawful access, resold to third parties and reused in other attack schemes, including phishing, a technique consisting of pretending to be an official body (social security body, bank, etc.) which requests, for example, its "prey" to confirm their banking data. In addition, these individuals are particularly exposed to risks of identity theft.

b) <u>On the grievance of insufficient strength of access passwords for the user interface</u>

71. The rapporteur notes that passwords allowing merchants to access their "client" area are stored with the SHA-1 hash function that is obsolete. It also notes that these passwords may be composed of only one character, which does not make it possible to ensure the security of the data to which they give access.

72. In its defence, the company explains that there was an error in the information initially supplied by [redacted] during the document monitoring. It indicates that the SHA-1 hash function is used only by the old user interface made available by [redacted] and currently in the process of decommissioning, and not the current interface. It specifies that access to this old interface has been revoked and that only two merchants still use this solution although [redacted] has duly notified them of the need to migrate to the new solution as soon as possible.

73. The company adds that the new solution uses the Bcrypt hash function recommended by CNIL to store passwords in a dedicated database. The latest version of the current interface embeds a so-called "anti-brute force" function, which incorporates multi-factor authentication and requires the use of a password of a length of 10 to 128 characters, comprising four types of characters (upper case, lower case, numbers and special characters).

74. The Restricted Committee first notes that, in its observations in response to the sanction report, the company sent information different from that communicated during the monitoring of documents concerning the hash function used for the storage of passwords allowing merchants to access their "client" area. The company thus indicated that the use of the obsolete hash function (SHA-1) concerns only the old user interface, which is being decommissioned, and which is used by two merchants. The Restricted Committee then notes that the two merchants in question have been given formal notice to migrate as soon as possible to the latest version of the interface, which uses a satisfactory hash function. Finally, the Restricted Committee observes that the elements of the case do not allow for calling into question the company's current statements.

75. The Restricted Committee therefore takes note of these statements and considers that there is no need to retain any breach relating to the security obligation due to insufficient strength of passwords for access to the user interface, allowing merchants to access personal data relating to their account.

3. On the breach of the obligation to notify data subjects of a personal data breach

76. Under Article 34 GDPR: *"1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

> *a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*

b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. […]".

77. Recital 86 of the GDPR provides that where the personal data breach is likely to result in a high risk to the rights and freedoms of the individual, the controller should communicate it to the data subject as soon as possible so that he or she can take the necessary precautions.

78. In this case, the rapporteur found that. following the data breach, the company [redacted], which has a "*procedure for handling personal data breaches*", considered that the risk related to the data breach was not high for the data subjects and that it therefore did not have to inform them.

79. The rapporteur considers, however, that, given the nature of the personal data, the volume of data subjects, the ease of identifying the persons affected by the breach and the possible consequences for the data subjects, the risk associated with the breach can be considered high and that communication to the data subjects should have been made.

80. In its defence, [redacted] indicates that it informed the merchants on whose behalf it had collected the data subject to the data breach at short notice, and that they were thus able, in their capacity as data controllers, to inform the data subjects if they considered it necessary.

81. The company also specified that, even though [redacted] processed the data for the purposes of reinforcing the fight against fraud as the controller, the data processed to this end was initially collected and processed by [redacted] as a processor on behalf of such merchants. It was therefore not possible to inform the debtors concerned directly without the agreement of these merchants.

82. In any event, the company considers that the format of the data and the circumstances surrounding the data breach led it to conclude that there was no high risk for the data subjects within the meaning of Article 34 GDPR, in light of the following elements:
    - The data format did not allow the nature or the content of the data to be understood directly; specific software was required;
    - no disclosure of data attributable to [redacted] has been established;
    - No identity theft or attempted theft has been reported to [redacted] by any debtor;
    - The nature of the data does not suggest that there was a high risk of financial fraud;
    - The risk to a data subject appeared to be ineffective insofar as any debtor has the right to oppose an unauthorised debit without justification for eight weeks, and for up to thirteen months after the transaction with justification.

83. The company further recalls that it did not have all the email addresses of the data subjects concerned. It therefore concludes that informing the debtors individually would have proved impossible for a large part of them. It also considers that a public communication would not have been relevant insofar as its services were offered to professional clients, the majority of

the debtors concerned would not have been able to determine whether or not their data had been processed by it, acting in a non-visible manner as a payment service provider.

84. **Firstly**, the Restricted Committee considers that [redacted]'s argument to avoid its liability, according to which the data on the basis of which the processing was carried out were initially collected and processed by [redacted] as a data processor on behalf of merchants, is not convincing. The fact that the data in question were initially processed for another purpose for which the company acts as a data processor does not affect its obligation under Article 34 GDPR to the extent that it has reused the data on its own behalf as a data controller.

85. **Secondly**, the Restricted Committee considers that, in view of the nature of the personal data (including banking information), the volume of data subjects (more than 12 million), the ease of identifying the persons affected by the breach and the possible consequences for the data subjects (risks of phishing and identity theft), the risk associated with the breach can be considered as high.

86. **Thirdly**, the Restricted Committee notes that Article 34-3 GDPR provides that communication to data subjects is not necessary in certain cases, particularly if the data controller has implemented appropriate technical and organisational protection measures, if it has taken further measures to ensure that the high risk to individuals is no longer likely to materialise or if it would require disproportionate efforts. The Restricted Committee considers that the company cannot avail itself of these provisions insofar as it has not implemented appropriate safeguards to ensure the security of the data affected by the breach (to limit their access to authorised persons only). Furthermore, while the company shut down the server concerned, the data remained accessible between November 2015 and February 2020, which is a very long period;

87. With regard to the company's argument that the informing all of the debtors individually would have required disproportionate effort, the Restricted Committee points out that the company had 6,250,310 e-mail addresses, or about half of the data subjects. It would, at the very least, have been able to inform those individuals of the data breach, without it constituting a disproportionate effort.

88. With regard to the company's argument that a public communication on its website would not have been relevant since the majority of the debtors concerned would not have been able to determine whether or not they had used [redacted]'s services, which intervene opaquely as a payment service provider, the Restricted Committee first notes that the company's website contains the names of some of its customers and that the debtors of these merchants could have been able to know that their data were potentially processed by [redacted] and possibly concerned by the breach. In this respect, it recalls that any natural person may exercise their rights provided by the GDPR with any company and thus obtain information on the question of whether or not their data are processed by said company. In the event of a public communication, the persons who so wish could therefore have contacted the company to find out if they were concerned by the data breach. Secondly, the Restricted Committee observes that information relating to a data breach of this magnitude can be retrieved on the web (social networks, newspapers and specialised sites, etc.). A public communication on the organization's website can thus be a starting point and the information can then take a much more significant dimension.

89. In view of these elements, the Restricted Committee considers that the company has failed to comply with its obligations under Article 34 GDPR, relating to the communication to data subjects of a personal data breach.

III. <u>On corrective powers and their publication</u>

90. Under Article 20 (III) of the amended French Data Protection Act of 6 January 1978, *"When the controller or his processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chairman of CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the restricted committee of the agency with a view to the announcement, after adversarial procedure, of one or more of the following measures:* […]

7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83".

91. Article 83 GDPR states that *"Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive"*, before specifying the elements to be taken into account when deciding whether to impose an administrative fine and to decide on the amount of that fine.

92. **Firstly**, on the principle of imposing a fine, the company maintains that such a measure is not justified. The company asserts that it has complied with its legal and regulatory obligations and that it has cooperated with CNIL in a diligent manner and in good faith since becoming aware of the security incident. It points out in particular that it notified CNIL of the data breach as soon as it became aware of it within the regulatory time-limit of 72 hours, had investigations carried out, making it possible to conclude that there was no risk to the rights and freedoms of the data subjects, implemented corrective measures very quickly, and informed the merchants concerned promptly.

93. The rapporteur recalls that in determining the amount of an administrative fine, the restricted committee must take into account the criteria specified in Article 83 GDPR, such as the nature, gravity and duration of the infringement, the measures taken by the controller to mitigate the damage suffered by the data subjects, the degree of cooperation with the supervisory authority and the categories of personal data concerned by the infringement.

94. Firstly, the Restricted Committee notes that the breaches affect a very large number of people, as the data breach involved more than 12 million debtors.

95. The Restricted Committee next considers that the accessible data (title, last name, first name, e-mail address, postal address, telephone number, BIC/IBAN) make it possible to obtain very precise information on the data subjects by revealing their identity and contact details. In addition, specific data are concerned, as some of them relate to financial information. The fact, in particular, that IBANs were included is not trivial. As stated by the Banque de France in its

work, “Payments and market infrastructures in the digital era”, IBANs are “*sensitive*” payment data (in the usual sense of the term) because they can be used to commit fraud. The European Data Protection Board describes this type of data as “*highly personal*”. The Restricted Committee considers that the company should have been particularly vigilant in securing such data, which can be reused by unauthorised third parties, thus harming the individuals concerned by the data breach. For example, they are at risk of identity theft or phishing, (i.e. sending fraudulent e-mails to obtain data) if their full identity, associated with their e-mail address for a large number of them, was freely available.

96. Lastly, the Restricted Committee finds that the data thus remained accessible for a very long period, between the end of the import of the data on the server in November 2015 and the discovery of the incident by the company on 14 February 2020, even though the processing concerned, the research project, had ended in July 2016. It is clear from the elements contained in the case file that, prior to the data breach, the company had not taken basic security measures. It was only through a report by a merchant that the company was made aware of the security failure.

97. While the Restricted Committee reveals that [redacted] immediately reacted to the data breach as soon as it was discovered in February 2020, and that it cooperated throughout the procedure with CNIL services, it considers that the data breach results from negligence of basic information systems security rules which led to making the personal data processed by the company accessible to unauthorised third parties.

98. The Restricted Committee points out that the negligence in terms of security was particularly serious: access to the server in question was not subject to any satisfactory access restriction, the company had not implemented any server access logging measures, and the data contained on the server could easily be read.

99. The Restricted Committee notes that this negligence is all the more serious in view of the business sector of the company, which prides itself on being the European leader in recurrent payments and is a company whose core business is the management of complex information systems.

100. The Restricted Committee also notes that, in disregard of Article 34 GDPR, the company did not inform the data subjects of the occurrence of the data breach, whereas it had more than 6 million e-mail addresses to do so, i.e., about half of the data subjects, and that it could have informed the remaining half by means of public communication on its site.

101. Lastly, the Restricted Committee recalls that the company had recourse to data processors acting under its authority as sub-processors vis-à-vis the merchants, for the services it provides to the latter, without having taken sufficient steps to ensure that the latter present the required guarantees and without having concluded contracts with some of them containing all the clauses provided for by Article 28 (3) GDPR.

102. Consequently, the Restricted Committee considers that an administrative fine should be imposed in view of the breaches of Articles 28, (3) and (4) GDPR, and 32 and 34 GDPR.

103. **Secondly**, with regard to the amount of the fine, the company considers that the amount proposed by the rapporteur is disproportionate in view of its economic situation. It insists on its

loss-making financial situation and specifies that a high fine would have a catastrophic impact on the jobs it is trying to sustain.

104. The Restricted Committee recalls that Article 83(3) of the Regulation provides that in the event of multiple breaches, as in the case in point, the total amount of the fine may not exceed the amount set for the most serious breach. Insofar as the company is alleged to be in breach of Articles 28, 32 and 34 GDPR, the maximum fine that can be imposed is 10 million euros or 2% of annual worldwide turnover, whichever is higher.

105. The restricted committee also recalls that administrative fines must be dissuasive but proportionate. In particular, it considers that the company's activity and financial situation must be taken into account when determining the penalty and, in particular, in the case of an administrative fine, its amount. It notes in this respect that the company reported turnover of [redacted] in 2019 and [redacted] in 2020, for [redacted] earnings of [redacted] in 2019 and [redacted] in 2020.

106. In view of these elements, the Restricted Committee considers that the imposition of a fine of €180,000 appears justified

107. **Thirdly**, with regard to the publication of the sanction, [redacted] argues that it is trying to make itself a place on a highly competitive international market of payment service providers, mostly dominated by Chinese and American companies, which are not concerned with European data protection. It adds that substantial efforts have been made for more than ten years to become a trusted partner for European economic players, stating that a public sanction would permanently prevent the results achieved through its efforts.

108. The Restricted Committee considers that the publication of the penalty is justified in view of the severity of breaches identified, their persistence, and the number of data subjects.

FOR THESE REASONS

CNIL's restricted committee after having deliberated, decides to:

- **impose an administrative fine of €180,000 (one hundred and eighty thousand euros) against [redacted];**

- **Make public, on the CNIL website and on the Légifrance website, its decision, which will no longer identify the company at the end of a period of two years following its publication.**

The Chairman

[redacted]

This decision may be appealed to the French Conseil d'Etat within two months of its notification.