4/28/2021
North Dakota Attorney General
600 E. Boulevard
Bismarck, ND 58503
ndag@nd.gov

Dear Sir/Madam:

We are outside counsel to ClearVoice Research.com, LLC ("ClearVoice") and are contacting you on its behalf. Pursuant to N.D. Cent. Code §§ 51-30-01 et seq. ("Law"), we are writing to notify you of a data security incident that permitted unauthorized access of personal information involving residents of the State of North Dakota.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

ClearVoice is a provider of market research services and maintains databases with the basic information of individuals who participate in their research projects and surveys. On April 17, 2021 at 16:50 EDT, ClearVoice received an e-mail from an individual (the "unauthorized user") stating he accessed a backup file of one of ClearVoice's old databases containing profile information of survey participants from 2015 that was publicly exposed in a storage container of our cloud service provider. ClearVoice uses a cloud service as its hosting provider and to store our databases and backups. A folder was created within this cloud service on September 17, 2015 to store database backups. The folder these backups resided in was, due to human error, accessible to any individual who (a) was provided the link to it or (b) could use an automated tool or other means to locate publicly open files.

Upon receipt of the information from the unauthorized user, ClearVoice immediately launched an investigation into the matter. Within an hour of receiving the email, ClearVoice located the backup file, secured it and eliminated any further exposure to the file. ClearVoice also conducted a comprehensive search of all of our databases and files and determined that no other files had been exposed and other files were properly secured. As part of the investigation, it was determined that the file contained weekly backups of a database from August and September of 2015.

Furthermore, even though the database had been accessible since 2015, according to log files that date back to the file's creation, the database has only been accessed twice, both times in the 24 hour period prior to when the unauthorized user notified ClearVoice of the exposed file, and thus such access was likely by the unauthorized user who contacted us on April 17, 2021.

On April 17, 2021, the backup files in the file storage service that had been inadvertently left unsecured due to a human error were properly secured. However, the data that was accessed by the unauthorized user appears to have been posted online, for purchase by the public.

DATA INVOLVED

The data comprises the following data categories of roughly 1,945 individuals: contact information from panel participants from 2015 (name, e-mail address, home address, phone number, date of birth), passwords from 2015, and, as applicable, responses to various questions the participants answered as part of their profile information on the ClearVoice platform which may include, but not be limited to, health condition, political affiliation, and ethnicity.

It is important to note that the data that was accessible did not include social security numbers, ID numbers, credit card numbers, other financial information, or data collected from specific surveys the participants may have taken part in.

POTENTIAL CONSEQUENCES OF THE INCIDENT

As the database was made publicly accessible by the unauthorized user, the accessibility of the information could be potentially used for unwanted contact intake or unwanted individual advertising measures. The information in some cases also contained responses to yes/no questions on various topics, which may include but is not limited to, the presence of general health conditions, political affiliation, and ethnicity. This information could be used to prepare personal profiles of the affected data subjects, which could possibly be used in a commercial or political context. Additionally, in the event passwords from 2015 are still being used by the individuals on other websites or platforms, unauthorized access to these accounts may occur.

STEPS TAKEN RELATING TO THE INCIDENT

As stated above, on April 17, 2021, ClearVoice has secured and eliminated any further exposure to the files in the file storage service that had been left unsecured due to the inadvertent human error. A thorough review of the system has been conducted and ClearVoice believes that the incident has been ully addressed. Additionally, ClearVoice forced a password reset for all persons that participate in the panels/surveys and members whose information had been potentially exposed in the backup file, and the credentials of all employees have been changed. ClearVoice has implemented additional security measures designed to prevent a recurrence of such an incident and to protect the privacy of panel participants.

In accordance with the Law, ClearVoice will send notification via secure e-mail to the affected residents on or about April 29, 2021, in substantially the same form as the letter attached hereto.

EXPLANATION FOR DELAY OF NOTIFICATION

There was a brief delay in providing notification, as the focus was on forensic work to ensure that the incident did not impact other data and to understand the full scope of the incident.

OTHER NOTIFICATION AND CONTACT INFORMATION

If you have any questions regarding this incident or if you desire further information or assistance, please call the undersigned at 303-473-2703 or email tbgray@hollandhart.com.

Sincerely,

Tracy B. Gray
Partner, Holland & Hart, LLP

Enclosure: Sample Breach Notification Letter
cc: ClearVoice

NOTICE OF DATA BREACH

Confidential-for Intended Recipient Only

Click or tap to enter a date.

Dear Click or tap here to enter text.,

We are contacting you regarding a data security incident we discovered on April 17, 2021 at ClearVoiceResearch.com, LLC ("ClearVoice"). You are receiving this notice because you have used ClearVoice to sign up for a profile to participate in market research surveys and your personal information was accessed. The privacy and protection of the personal information of our survey respondents is a matter we take very seriously, and we recommend that you closely review the information provided in this notice for suggestions on how to protect yourself against potential misuse of your information.

1. What Happened?

On April 17, 2021, we received an e-mail from an individual ("unauthorized user") stating he accessed a backup file of one of our databases containing profile information of survey participants from August and September of 2015. This database was later discovered to have been posted online, for purchase by the public.

2. What Data Was Affected?

The data that was accessible may include the following: contact information from 2015 (name, e-mail address, home address, phone number, date of birth), passwords from 2015, and, as applicable, responses to various questions you may have answered as part of creating your profile on our platform which may include, but not be limited to, health condition, political affiliation, and ethnicity.

It is important to note that the data that was accessible did not include national insurance numbers, social security numbers, ID numbers, credit card numbers, other financial information, or data collected from specific surveys you may have taken part in.

3. What Are Potential Consequences To You?

It cannot be ruled out that the data sets mentioned above can be misused and you may be contacted by for advertising purposes or similar. Further, it cannot be excluded that the accessible information could be used to prepare personal profiles, which could possibly be used in a commercial or political context.

4. What We Are Doing.

Upon receipt of the information from the unauthorized user, we immediately launched an investigation into the matter. Within an hour of receiving the email from the unauthorized user, we located the backup file, secured it and eliminated any further exposure to the file in the cloud service. We also conducted a comprehensive search of all of our databases and files and determined that no other files had been exposed and other files were properly secured. We will continue to take steps necessary to minimize any disruption that this compromise may have caused and to prevent such incidents in the future. Furthermore, ClearVoice forced a password reset for all persons that participate in our panels and members whose information had potentially been exposed. Further, ClearVoice has implemented additional security measures designed to prevent a recurrence of such an incident and to protect the privacy of your data.

5. What You Can Do.

Given the types of information that was accessible as part of this incident, we do not believe that there is a risk of identity theft from this incident. However, we encourage you to take usual prudent precautions with your personal information. You should not open email or text messages from any unknown sender. You should never open untrusted web links. You should never provide personal information via email or over the phone to any unverified entity. If you continue to use the same password as in 2015, even for other accounts or platforms, there is a risk that an unauthorized access of your accounts may occur, and you should change your password settings of those other accounts respectively.

6. For More Information.

We have set up a webpage https://hosted.clearvoicesurveysmail.com/FA32/ to provide information, which will be updated, as additional information becomes available. If you have further questions regarding this incident, please email us at datainquiries@clearvoiceresearch.com.

We truly apologize for this incident and regret any inconvenience to our panel participants.

Sincerely,
The ClearVoice Research Executive Team