From: [redacted]
To: [redacted]
Subject: [redacted]
Date: [redacted]

[redacted]

From: Jessica G <jessica@clearview.ai>
Sent: Tuesday, February 25, 2020 3:03 PM
To: Jessica G <jessica@clearview.ai>
Subject: Clearview Statement to Customers

Statement to our Customers:
We are writing to let you know that someone has gained unauthorized access to our organization list. They retrieved the following:
* Organization Names
* Number of user accounts
* Number of searches

No passwords or any personally identifiable information of customers were revealed. While some information about test user accounts may have been accessed, no law enforcement search histories, emails, user names, public photos or any biometric data were accessed.

Our servers were not breached, and there was no compromise of Clearview's systems or network.

Most importantly, we have fixed this vulnerability. We are contacting the authorities about this unauthorized access.

If you have any questions, please feel free to contact us at: help@clearview.ai

Thank you,
Team Clearview

Jessica Medeiros Garrison
205.568.4371
jessica@clearview.ai

From: [redacted]
To:
Subject:
Date:

[redacted]

From: Jessica G <jessica@clearview.ai>
Sent: Wednesday, February 26, 2020 1:20 PM
To: JIMMY CHAN <jichan@smcgov.org>
Cc: Jordan Newell <jnewell@smcgov.org>; Ana Bueno-Moran <ABueno-Moran@smcgov.org>; Jack M <jack@clearview.ai>
Subject: Re: Clearview Breach

Good afternoon. Here are the responses to your inquiry.

1. Is it just our agency's name or does that include any other type of information (such as contact person for our agency, phone number, address, etc.)?
    a. Just your agency's Name "San Mateo County (Ca)"
    b. No law enforcement search histories, names, phone numbers or emails were accessed or accessible.

2. By "Number of user accounts", does that mean the number of user accounts Clearview has licensed or the number of user accounts our agency has with Clearview?
    a. Number of user accounts each agency has with CV

3. By "Number of searches", does that mean the total number of searches that has gone through Clearview by ALL customers as a whole or the total number of searches performed by each individually named organization?
    a. Total Number of searches collectively of all users in each agency (2700+ searches)

4. Was this breach an individual computer/laptop, cloud storage, networked drive, via a firewall intrusion, paper files, unauthorized building/premise access?
    a. The attacker obtained unauthorized access to an internal Clearview test account and was able to use that to exfiltrate the information.

5. What security protocols/procedures/policy has been put into place to address the vulnerability that was present that allowed the breach?
    a. We have shut down the test account that was compromised, initiated a full

cybersecurity review, and we're improving various systems that make it more difficult to analyze the Clearview app, and reducing risks associated with an account takeover.

Jessica Medeiros Garrison
205.568.4371
jessica@clearview.ai

From: JIMMY CHAN <jichan@smcgov.org>
Date: Wednesday, February 26, 2020 at 9:13 AM
To: "jessica@clearview.ai" <jessica@clearview.ai>
Cc: Jordan Newell <jnewell@smcgov.org>, Ana Bueno-Moran <ABueno-Moran@smcgov.org>
Subject: Clearview Breach

Jessica,

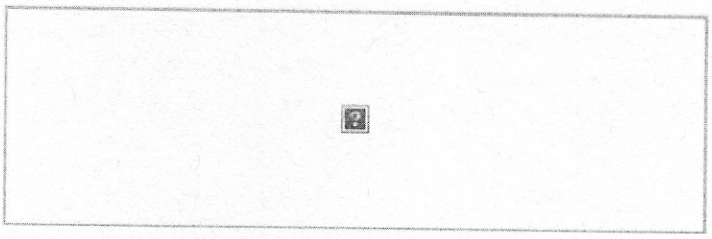
As clarification regarding your breach, our agency would like to know exactly what data was compromised. You listed in your initial email that the following was accessed by the unknown "hacker(s)":

* Organization Names
* Number of user accounts
* Number of searches

Can you advise further in regards to the following:

1) Is it just our agency's name or does that include any other type of information (such as contact person for our agency, phone number, address, etc.)?
2) By "Number of user accounts", does that mean the number of user accounts Clearview has licensed or the number of user accounts our agency has with Clearview?
3) By "Number of searches", does that mean the total number of searches that has gone through Clearview by ALL customers as a whole or the total number of searches performed by each individually named organization?
4) Was this breach an individual computer/laptop, cloud storage, networked drive, via a firewall intrusion, paper files, unauthorized building/premise access?
5) What security protocols/procedures/policy has been put into place to address the vulnerability that was present that allowed the breach?

Your response to the questions are necessary for us to answer inevitable questions that will follow from our Command Staff and to help formulate a response to any media/public relations query that will be forthcoming.



From: [redacted]
To:
Subject:
Date:

[redacted]

From: Hoan T <hoan@clearview.ai>
Sent: Thursday, February 27, 2020 1:10 PM
To: JIMMY CHAN
Subject: Clearview responses

CAUTION: This email originated from outside of San Mateo County. Unless you recognize the sender's email address and know the content is safe, do not click links, open attachments or reply.

Is it just our agency's name or does that include any other type of information (such as contact person for our agency, phone number, address, etc.)?

- Just your agency's Name "San Mateo County (Ca)"
- No names/emails/phones were compromised.

- By "Number of user accounts", does that mean the number of user accounts Clearview has licensed or the number of user accounts our agency has with Clearview?
  - Number of user accounts the agency has with CV

- By "Number of searches", does that mean the total number of searches that has gone through Clearview by ALL customers as a whole or the total number of searches performed by each individually named organization?
  - Total Number of searches collectively of all users (2700+ searches)

- Was this breach an individual computer/laptop, cloud storage, networked drive, via a firewall intrusion, paper files, unauthorized building/premise access?
  - It was from stolen account credentials of a test account

- What security protocols/procedures/policy has been put into place to address the vulnerability that was present that allowed the breach?
  - We are adding two-factor authentication and already have implemented email alerts when a login happens