[July 23, 2020 Email notification to affected individuals]

Information regarding data protection following data breach

Dear Slidely and Promo community,

I'm writing to notify you about a targeted breach of some of our servers which hold some of our customers' account information but do not include any financial data. Whilst the issue has been identified and resolved, we continue to work closely with cybersecurity experts and relevant authorities and have already implemented further security measures and features.

This message provides important information. We would like to apologise sincerely for the inconvenience caused.

What we know

On July 21, 2020, our team became aware that a data security vulnerability on a third-party service which affected many companies had caused a breach affecting certain non-finance related Slidely and Promo user data. We immediately launched an internal investigation to identify what had occurred and to take all necessary steps to protect our customers.

What information was involved

First and foremost, **no financial data** such as credit cards or billing information, **was accessed as we never store this information on our servers**.

The breached servers held the following data: first name, last name, email address, IP address, approximated user location based on the IP address, gender, as well as encrypted, hashed and salted passwords to Slidely and Promo. Your account password was hashed and salted (a method used to secure passwords with a key), however, it is possible that it could subsequently have been decoded.

What we are doing about it

We have acted immediately and are taking this incident and the security of your information extremely seriously. We are protecting you and the rest of our community in the following ways:

- We are sending you this update with recommendations on what you should do
- We have completely removed the vulnerable third-party service from our platform
- We've hired a leading cybersecurity specialist to further review and reinforce our protections
- We continuously enhance our safeguards and systems that detect and prevent unauthorized access to user accounts

What you should do

As an immediate precautionary measure, you should reset the password to your Slidely or Promo account as soon as possible. To do so, please use this link: https://promo.com/forgot and follow the instructions there.

Also, if you have been using the same or a similar password for other online accounts, **we strongly recommend you change those passwords** to protect those accounts as well. For your convenience, please check out the best practices here**.**

For more information

Should you want any additional information or would like to connect with our team contact us at support@promo.com. We are working around the clock and are here to help and support you.

Your sincerely,

Tom More, CEO

[September 6-7, 2020 Email notification to affected individuals]

Title: Follow-up Notice of Data Breach

September [6/7], 2020

Dear Slidely and Promo community,

Following our initial email to you on July 23, about a targeted breach of some of our servers which hold some of our customers' account information but do not include any financial data, I am writing to provide further important information.

First, we would again like to apologise sincerely for the inconvenience caused. As we mentioned in our earlier email on July 23, he issue has been identified and resolved and we continue to work closely with cybersecurity experts and relevant authorities and have already implemented further security measures and features.

What Happened

On July 21, 2020, our team became aware of a data security vulnerability on a third-party service which affected many companies. This caused a breach that occurred between June 22-25, affecting certain non-financial related Slidely and Promo user data. We immediately launched an internal investigation to identify what had occurred and took all necessary steps to protect our customers.

What information was involved

First and foremost, **no financial data** such as credit cards or billing information, **was accessed as we never store this information on our servers**.

The breached servers held the following data: first name, last name, email address, IP address, approximated user location based on the IP address, gender, as well as encrypted, hashed and salted passwords to Slidely and Promo. Your account password was hashed and salted (a method used to secure passwords with a key); it is possible, however, that it could subsequently have been decoded.

What we are doing

We acted immediately. We are taking this incident and the security of your information extremely seriously. We are protecting you and the rest of our community in the following ways:

- We are sending you this update with recommendations on what you should do
- We have completely removed the vulnerable third-party service from our platform
- We've hired a leading cybersecurity specialist to further review and reinforce our protections
- We continuously enhance our safeguards and systems that detect and prevent unauthorized access to user accounts

What you can do

As a precautionary measure, you should reset the password to your Slidely or Promo account as soon as possible if you haven't done so already. To do this, please use this link: https://promo.com/forgot and follow the instructions there.

Also, if you have been using the same or a similar password for other online accounts, **we strongly recommend you change those passwords** to protect those accounts as well. For your convenience, please check out the best practices here**.**

No financial data, such as credit cards or billing information, was accessed as we never store this information on our servers, but government agencies generally advise that consumers remain vigilant by reviewing account statements and monitoring free credit reports. You can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

- A Security Freeze prevents most potential creditors from viewing your credit reports and therefore, further restricts the opening of unauthorized accounts.
- A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts

For more information:

- New York Department of State Division of Consumer Protection: http://www.dos.ny.gov/consumerprotection (Consumer Helpline: (800) 697-1220)
- NYS Attorney General at: http://www.ag.ny.gov/home.html
- Federal Trade Commission at: www.ftc.gov/bcp/edu/microsites/idtheft/ (Helpline: 1-877-438-4338). 600 Pennsylvania Avenue, NW, Washington, DC 20580

Credit reporting agencies:

- Equifax: www.equifax.com or 1-800-685-1111.
  Equifax Information Services LLC

P.O. Box 105788 Atlanta, GA 30348-5788

- Experian: www.experian.com or 1-888-397-3742
  475 Anton Blvd.
  Costa Mesa, CA 92626
- TransUnion: www.transunion.com or 1-888-909-8872
  P.O. Box 160
  Woodlyn, PA 19094

For more information

Should you want any additional information or would like to connect with our team contact us at support@promo.com. We are working around the clock and are here to help and support you.

Your sincerely,

Tom More, CEO