Subject: Docsketch security related message

In early August, we discovered suspicious activity in a three-week old copy of our primary database. We immediately investigated and found that an unidentified attacker accessed the database. This is something we take very seriously and we want to be transparent about what happened and how we're handling this.

What happened?

An unauthorized third party accessed a three-week old copy of our database containing data from July 9, 2020 and before. This database contained contact information and form fields related to documents filled out by users and users' recipients.

The documents themselves were not accessed by this unauthorized third party.

What information was involved?

The data accessed includes July 9, 2020 (and older) login information and contacts. Passwords were not stored in plain text, but rather are protected using a form of one-way encryption (called 'salting and hashing').

While the documents themselves were not accessed, the completed fields for documents (July 9th and before) were compromised as well. This means that if you have documents with text fields that you or someone else has filled out, those were part of the data breach.

What we are doing

As soon as we discovered the incident, we immediately took steps to secure our systems and prevent further access. We enhanced security around documents, document data encryption, and more.

Our infrastructure has already been upgraded in a way that prevents this type of access from happening in the future.

We are currently working with outside infrastructure and security firms on future enhancements and upgrades, including moving towards SOC 2 compliance.
We're still working out the details but rest assured this is our top priority and we're going to continue making significant security and infrastructure updates.

What you can do

Docsketch has already notified every affected user and document recipient with a valid email address, but if you have specific questions about this you can contact us by replying to this notice. Please also review this Addendum for additional suggested next steps.

A sincere apology

We're truly sorry about this. I—and the entire Docsketch team—appreciate the trust you put in us. This isn't something we take lightly and we appreciate your patience as we work through this unfortunate incident.

Moving forward, we'll continue working hard and making significant investments on security and our infrastructure.

If you have any questions or concerns about anything that I've mentioned, please reply back to this email.

Sincerely,

Ruben Gamez
Founder, Docsketch

Addendum - Next Steps

Credit Card Information

If you believe the fields you completed in documents contained credit card information, you should take steps to secure your credit account by taking the following steps:

- Review your card statements for the affected credit card and look for unauthorized transactions;
- Obtain and review your annual credit report;
- Consider placing a “freeze” on your credit with the major consumer credit reporting bureaus; and
- Notify your card-issuing bank if you discover any fraudulent activity.

Social Security Numbers

If you believe the fields you completed in documents contained information related to your personal identity, you should take steps to protect your credit and personal identity:

- Obtain and review your annual credit report;
- **Security Freeze.** In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national

credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.