



<Sent via electronic mail at IDTheft@oag.state.md.us and consumer@oag.state.md.us>

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

September 7, 2023

Re: Practice Suite, Inc. Data Breach

To Whom It May Concern:

My name is David Heller and I represent PracticeSuite, Inc. ("Practice Suite"). I am writing you to provide you of notice of a data breach that has affected five (5) residents of Maryland. It has affected four customers of PracticeSuite and one employee. This correspondence summarizes the data breach and Practice Suite's current response to it. Maryland residents who are customers have been or will be notified by mail on September 7, 2023. Maryland residents who are employees will be notified early next week, but will be offered the same benefits outlined in the customer-facing communication. A template copy of that correspondence is attached for your reference.

a) Summary

Practice Suite offers software-as-a-service to its customers, who are healthcare practices. When a customer enrolls in Practice Suite's services, they fill out a credit authorization form, and a general enrollment form. An employee's email was recently compromised and monitored by an unauthorized third party ("UTP"). The employee belonged to the accounting and billing department. That department manages day-to-day billing and processing these initial forms. While this employee did not receive initial forms as a matter of course, when she received questions regarding an account, she would sometimes receive information contain in such forms from other Practice Suite employees or customers themselves. In addition, she received employee benefit enrollment forms.

b) The method of data breach.

The UTP used email phishing to obtain the email credentials ("the Credentials") of a Practice Suite employee.

c) The approximate date and time of the data breach.

The UTP obtained the Credentials on June 19, 2023. They potentially monitored and/or accessed the employee's emails from that period until July 14, 2023.

d) The approximate number of files compromised as a result of the data breach.

Two individuals in Maryland were affected. One is an employee of PracticeSuite, the other a customer.

e) A detailed description of the type and nature of the information that was compromised.



With respect to the affected customer(s), the email address belonged to a member of Practice Suite's Accounting and Enrollment department. We are still determining the extent to which certain data is exposed. Enrollment data includes the following data:

- Company name or practice name;
- Name on credit card/debit card;
- Billing address;
- Phone number;
- Credit card number;
- Expiration date;
- Card cvv/cvc; and,
- Any other information submitted to Practice Suite during the customer's enrollment in Practice Suite's services; any other information used on a customer's for credit card authorization form.

PracticeSuite's customers, although business's, often use personal credit cards to make payment to PracticeSuite. That is the case with respect to the affected resident(s) in Maryland.

With respect to the affected employee(s), the enrollment form would have included the following data:

- Social security number;
- Date of birth;
- Personal addresses; and,
- Bank information (e.g. checking/saving account numbers and routing numbers).

f) Discovery and Practice Suite's ongoing investigation

Practice Suite has initiated an investigation to determine the scope of the breach, any immediate remediation measures it should take, and any strategic security changes it should make. On July 13, 2023, a Practice Suite customer called Practice Suite and notified it that an individual had contacted the customer with new payment instructions for that customer's monthly subscription payment to Practice Suite. The customer submitted payment through to the account that the hacker provided the customer. Practice Suite informed the customer that it did not change its billing information, and coordination with the customer's bank to reverse the payment. As a result, Practice Suite initiated an investigation to determine the root cause of the issue. On around August 14, 2023, Practice Suite, through its investigation, found that personally identifiable information was part of the email content of the email address may have been exposed by a phishing scam perpetuated upon one of Practice Suite's employees. The investigation is ongoing.

g) Who received the information contained in the "data breach."

This information is not available at the time of this writing.

Please let me know if you have any comments or questions. I can be reached by email at dheller@davidhellerlaw.com, or by phone at 813-397-8250. I will provide further updates as they become available. Thank you for your time and consideration.

Sincerely,

David Heller, Esq.

September 7, 2023

RE: Important Data Breach Notification

We are reaching out regarding an important incident that may affect your privacy. Please review this correspondence in detail.

What happened?

On August 14, 2023, we discovered that an email account of one of our employees had been compromised by a third party which contained customer contracts and practice enrolment forms. Immediately, we manually reviewed the contents of the inbox to identify if these documents included any sensitive information. Pursuant to this intensive internal investigation, on September 4, 2023, we discovered your practice's credit card authorization form may have been exposed. Although, at this time we do not have any reason to believe that your specific information has been accessed or used. As a responsible company, we have taken immediate steps to remedy the situation. I want to assure you that we take your data security very seriously. We further recommend you take the steps outlined in this letter. To summarize, any information that you may have submitted as part of your credit card authorization form when you enrolled with PracticeSuite may be exposed and potentially compromised. That information includes the following:

- Company name or practice name;
- Name on the card;
- Billing address, phone number;
- Credit card number, expiration date, cvv/cvc code;
- Email address;
- Tax identification number provided (e.g. federal employer identification number ("FEIN")); and,
- Any other information that you may have submitted as part of enrollment to receive services from PracticeSuite.

What if I used a business credit card?

We will reimburse your business for credit monitoring for two years. To help protect your identity, we will reimburse you for a two-year membership of Experian's Business Credit Advantage. You can register online at the following link: <https://www.experian.com/small-business/monitor-business-credit>. This offer must be used within 90 days from the date of this letter. This must be used within 90 days of the date of this letter. After you register there, please contact us at compliance@practicesuite.com or call our support line at 813-607-2800. Your reimbursement code is "ZW34562Q." If you have questions about the product, please contact Experian's customer care team at 1-888-397-3742.

We ask that you be vigilant in reviewing your account statements and credit cards for any suspicious and/or unauthorized activity and that you are diligent in monitoring your credit reports for any unexplained activity. You may also want to report the potential breach to your credit card company. If your business's identity or credit has been compromised occurred you should report the incident to local law enforcement or your state attorney general's office. You should also place a fraud alert on your business credit. You can place one with Experian or Transunion by following the instructions on their website at the following links:

- <https://www.businesscreditfacts.com/pdp.aspx?pg=how-can-i-place-a-fraud-alert-on-my-business-credit-file>
- <https://www.transunion.com/product/business-fraud-alerts>

What if I used a personal credit card and not a business credit card?

First, to help protect your identity, we will reimburse you for a two-year membership of Experian's® IdentityWorksSM. This product provides you with identity detection and resolution of identity theft. We will reimburse you for a two-year membership with Identityworks. This offer must be used within 90 days of the date of this letter. Visit <https://www.experian.com/protection/compare-identity-theft-products/> and select the Premium Plan for \$24.99 per month. After you register there, please contact us at compliance@practicesuite.com or call our support line at 813-607-2800 and we will reimburse you. Your reimbursement code is "ZW34562Q." If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-888-397-3742.

Next, you also have the option of placing a fraud alert on your credit file. 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. Placing a fraud alert is easy – you contact any one of the three nationwide credit reporting agencies (Equifax, Experian, TransUnion) and that one will notify the other two. You can contact any one of the following:

- Equifax: by calling (800) 525-6285; or download the following form to request a fraud alert by mail. https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf
- Experian: by calling (888) 397-3742 or by going to: <https://www.experian.com/ncaconline/fraudalert>
- Transunion: by calling (800) 680-7289 or by going to <https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp>

Finally, you may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, send a written request by regular, certified or overnight mail to the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094
--	--	---

1-800-349-9960 https://www.equifax.com/personal/help/place-lift-remove-security-freeze/	1-888-397-3742 https://www.experian.com/freeze/center.html	1-888-909-8872 https://www.transunion.com/credit-freeze
---	---	---

As another step, you can obtain a free credit report by logging into www.annualcreditreport.com. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot a problem and address it quickly.

We sincerely apologize for this incident and regret any inconvenience it may cause you. We are taking all necessary steps to address this breach promptly and responsibly. We continue to review and enhance our security measures to fortify our systems, safeguard your information, and prevent similar incidents from occurring in the future. We are committed to supporting you throughout this process. If you have any questions, concerns, or require further assistance, please reach out to us at compliance@practicesuite.com or call our support line at 813-607-2800.

Sincerely,

Vinod Nair, CEO

PracticeSuite, Inc.