Pruitt-Hamm Law and Mediation Services, P.S.

Bruce Pruitt-Hamm, JD
Attorney and Counselor at Law
Certified Mediator
Certified Collaborative Professional

6013 29th Ave NE
Seattle, WA 98115
206-327-9335
Fax 866-566-7277
Email: bruce@pruitthammlaw.com
Website: www.pruitthammlaw.com

Dorinda C. Robinson
Paralegal
Carolyn Monet
Bookkeeper

August 24, 2020

Washington Attorney General's Office
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Sent to:SecurityBreach@atg.wa.gov

Re: Notification of Security Breach

To Whom It May Concern:

I am writing on behalf of Pruitt-Hamm Law and Mediation Services, PS ("PHLAMS") to inform you that we have recently become aware of a data security incident. The breach involved an unknown threat actor's ("hacker's") unauthorized access into the email account of the PHLAMS bookkeeper where the hacker set up a rule to forward certain emails from the bookkeeper to a third party phantom email address of the hacker (exec@cnilco.com).

These emails included information stored for many of PHLAMS clients' cases and personnel information. The breach occurred sometime before 5/22/2020 and 8/19/2020 (the date the breach was discovered by out IT provider). In the initial investigation that followed PHLAMS found only 2 emails that had been rerouted to the hacker contained "personal information" (social security number and WDL numbers, with first name and last name) for 2 of PHLAMS' staff. Based on further analysis of those files, the hacker potentially accessed information such as client names, mailing addresses, email addresses, and/or other potentially personal information. PHLAMS is unable to estimate the total number of affected Washington residents at this time, but it is currently only 2 who we know have had "personal information" disclosed to the hacker. This is less than 500 residents. Nonetheless, we are complying with the notice requirements of RCW 19.255.010 while we continue our investigation because of the potential risk of harm to our clients, vendors and staff.

PHLAMS is working with external cybersecurity experts to investigate this incident further, address any vulnerabilities, and remediate the incident. The external cybersecurity experts have taken steps to secure PHLAMS systems and networks at multiple levels to provide defense in depth. Advanced active monitoring and threat detection systems are also in use to detect and thwart potential attacks and identify suspicious behavior.

Please find enclosed a copy of the notification that will be sent to the affected individuals beginning Friday, August 21, 2020.

Please contact me at the above address with any questions or concerns regarding this incident.

Bruce Pruitt-Hamm, JD; WSBA #24005

Enclosure

Pruitt-Hamm Law and Mediation Services, P.S.

Bruce Pruitt-Hamm, JD
Attorney and Counselor at Law
Certified Mediator
Certified Collaborative Professional

6013 29th Ave NE
Seattle, WA 98115
206-327-9335
Fax 866-566-7277
Email: bruce@pruitthammlaw.com
Website: www.pruitthammlaw.com

Dorinda C. Robinson, Janice Dahl
Paralegals
Carolyn Monet
Bookkeeper

«Today_Date»

«People_Full_Name»
Sent to: «People_Primary_Email»

Dear «People_First_Name»:

Notice of Data Breach

What Happened?
We are contacting you because Pruitt-Hamm Law & Mediation Services, PS ("the Firm") learned on 8/19/20 of a data breach security incident that occurred on or before 5/22/2020 and continued until 8/19/2020 that may have involved some of your personal information. According to the Center for Victim Research, 7-10% of the U.S. population are victims of identity fraud each year.[1] The number of publicly reported data breaches increased 54% in the first half of 2019, compared to the same period in 2018.[2] We provide this information so you can better protect yourself, given the increasing frequency of this type of crime.

What Information Was Involved?
The incident involved an unknown threat actor ("hacker") who gained unauthorized access to our Firm's bookkeeper's email program on or before 5/22/20 and set up a rule to forward all her outgoing email to the hacker's phantom email address. Firm information, including invoices to our clients and personnel information was included in emails sent by the bookkeeper. The hacker potentially accessed information such as client names, emails and mailing addresses. Some emails included client credit card receipts, but those only include the last 4 numbers of the credit card account and are not included in the legal definition of "personal information". So far, our investigation has only revealed "personal information" for 2 of our staff as having been rerouted to the hacker in an attachment to an email.

What Are We Doing?
We have investigated the incident and taken the necessary steps to prevent it from recurring as well as mitigate its effect on you. We are continuing to investigate and will take further security measures as recommended by our cybersecurity experts.

We have reported this crime committed against our Firm to the Federal Bureau of Investigation (FBI) and Seattle Police Department. We are notifying you so you can take action along with our efforts to minimize or eliminate potential harm. Because this is a serious incident, we strongly encourage you to take preventive measures now to help prevent and detect any misuse of your information.

We are also notifying you even though it appears we are not legally required to do so per the terms of RCW 19.255. It does not appear that the law applies to this incident with the information we have so far (only 2 staff, i.e. fewer than 500 Washington residents) whose "personal information" was disclosed to the hacker. Nonetheless, we have submitted a

[1] https://www.consumeraffairs.com/finance/identity-theft-statistics.html
[2] https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

report to the Washington Attorney General's office per RCW 19.255.010 and are notifying all our current and past clients, vendors and employees who appear may have been impacted.

What You Can Do
Even though to date we have not received any reports of actual misuse of any information as a result of this incident, we recommend that you monitor your financial statements and credit reports for fraudulent transactions or accounts. If you see any unauthorized activity, promptly contact your financial institution.

In addition, you should NOT pay any invoice that appears to come from the Firm by means of online Internet payment. We do take credit cards, but always do it over the phone, not via direct payment over the Internet. It is possible the hacker may try to copy our invoice to appear legitimate and then direct you to pay via the Internet. If so, be advised this is not us. Contact us directly by phone if you have any questions or concerns (no charge), so we can clarify the situation for you.

You may obtain a free copy of your credit report maintained by each of the three credit reporting agencies by visiting www.annualcreditreport.com or by calling toll-free 877-322-8228. Review the reports carefully, and if you find anything you do not understand or that is incorrect, contact the appropriate credit reporting agency. Credit reporting agencies must investigate your report, and remove inaccurate, incomplete, or unverifiable information. In addition, if you suspect fraudulent activity, you can contact your local law enforcement agency, the attorney general of your state, and the Federal Trade Commission.

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. A victim's personal information is sometimes held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

You may also consider contacting the credit reporting agencies directly if you wish to put in place a fraud alert or a security freeze. A fraud alert will notify any merchant checking your credit history that you may be the victim of identity theft and that the merchant should take additional measures to verify the application. Contacting any one of the three agencies will place an alert on your file at all three. A security freeze restricts all creditor access to your account, but might also delay any requests you might make for new accounts. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. Enquire with the credit reporting agencies for their specific procedures regarding security freezes. Credit freezes are free.

- Equifax: 1-800-525-6285; P.O. Box 740241, Atlanta, GA 30374-0241; www.equifax.com/personal/credit-report-services/
- Experian: 1-888-EXPERIAN (397-3742); P.O. Box 9532, Allen, TX 75013; www.experian.com/help
- TransUnion: 1-800-680-7289; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790; www.transunion.com

On behalf of the Firm, we regret any inconvenience this may cause you. Working together, businesses and consumers can blunt the impact of cyber-crime.

Very truly yours,

Bruce Pruitt-Hamm, JD

Additional Information

IF YOU ARE A WASHINGTON RESIDENT: **You may also obtain information about avoiding identity theft from the Washington Attorney General's Office. This office can be reached at:**
Office of the Attorney General
Consumer Protection Division
800 Fifth Ave., Suite 2000
Seattle, WA 98104
https://www.atg.wa.gov/identity-theftprivacy

The Federal Trade Commission also provides information about how to avoid identity theft and what to do if you suspect your identity has been stolen. Visit identitytheft.gov, or write to Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580.