[redacted]

From: Gina Ulery <gina@pdresources.org>
Sent: Thursday, August 29, 2024 2:20 PM
To: IDTheft
Subject: Security Breach Notification
Attachments: Notice of Security Breach - MD.pdf

[redacted]

[redacted]

[redacted]

Good afternoon,

I am writing to inform the Maryland OAG of a security breach that may have affected 97 Maryland residents. My company, Professional Development Resources, provides online continuing education courses to healthcare professionals throughout the United States. A brief description of the security breach is provided below:

On 8/9/2024 we were contacted by Wells Fargo Merchant Services and notified about a possible digital skimmer on our website (https://www.pdresources.org/). We immediately contacted our website developers to verify (determined true) and implemented a patch. The alert from Wells Fargo stated "there are (5) affected payment cards with subsequent fraud totaling $1,240.00. The period of possible compromise started on 08/01/23 through 01/05/24."

Our website developers determined that the CC skimmer only targeted customers at checkout and sent requests to domain xu3.gay passing billing information and credit card details. They also found that our site was breached through our admin portal and so we have deleted all inactive users, changed passwords for active ones, and implemented two-factor authentication at login.

We filed a report with the FBI (ic3.gov) on 8/12/2024 and are working with a Cybersecurity Legal Officer to ensure that all state requirements are met in addition to enhancing our cybersecurity going forward.

A sample copy of the notification is attached.

Sincerely,
Gina Ulery

Gina Ulery, MS, RDN, LDN
President | Professional Development Resources
Earn CE Wherever YOU Love to Be **@pdresources.org**

Notice of Security Breach (Maryland Residents)

Dear (firstname),

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information.

What Happened:

On August 9, 2024, we were identified as a Common Point of Purchase (CPP) of 5 affected payment cards now experiencing fraud. We instantly investigated and found that an unauthorized individual gained access to our admin system and installed a digital skimmer on our checkout page, providing access to your billing and credit card information.

What We Are Doing:

We immediately took steps to secure our systems and prevent further unauthorized access. We have also engaged a leading cybersecurity firm to assist in our investigation and to enhance our security measures. Additionally, we have notified law enforcement and are cooperating with their investigation.

What You Can Do:

To protect yourself from potential misuse of your information, we recommend that you monitor your accounts for any suspicious activity and/or call your bank or credit card issuer and change your account numbers (if you are unsure which card(s) you have used on our website, please reply and I will find that information for you).

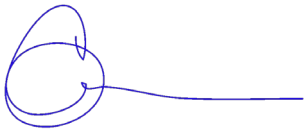
The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year and you can renew it after one year. You can also obtain information from these sources about steps to avoid identity theft:

* Equifax: (800) 685-1111 or https://www.equifax.com/
* Experian: (888) 397-3742 or https://www.experian.com/
* TransUnion: (888) 909-8872 or https://www.transunion.com/

We sincerely apologize for any inconvenience or concern this incident may cause you. Protecting your information is a top priority for us, and we are committed to preventing such incidents in the future.

If you have any questions, please reply to this email or contact our support team at help@pdresources.org or 1-800-979-9899. Additional resources are provided below.

Your friend in CE,



Gina Ulery, MS, RDN/LDN

President/CEO
Professional Development Resources, Inc.
PO Box 550659
Jacksonville, FL 32255-0659
gina@pdresources.org

Additional Resources:

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
(410) 528-8662
https://www.marylandattorneygeneral.gov/

Federal Trade Commission (FTC)
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
https://www.ftc.gov/

Equifax
P.O. Box 105283
Atlanta, GA 30348-5283
(800) 685-1111
https://www.equifax.com/

Experian
P.O. Box 9530
Allen, TX 75013
(888) 397-3742
https://www.experian.com/

TransUnion
P.O. Box 6790
Fullerton, CA 92834
(888) 909-8872
https://www.transunion.com/