

LAW OFFICES OF DANIEL D. KIM

Attorneys at Law
416 E. Central Blvd., 2nd Fl.
Palisades Park, NJ 07650

Tel. (201) 947-2188 Fax. (646) 349-1732 E-mail: danielkimlaw@gmail.com

New York Office
5 Penn Plaza, 23rd Fl.,
New York, New York 10001

June 19, 2023

Via E-Filing
Anthony G. Brown
MD Attorney General

Re: Client: iottie Inc
Breached website: www.iottie.com
Date of Breach: 4/12/23 thru 6/2/23
Discovery Date: June 13, 2023
Notice Date to Customers: June 19, 2023

To Whom It May Concern:

Please be advised that we represent iottie Inc., whose website was compromised on April 12, 2023. On June 13, 2023, iottie's cyber technician discovered that unauthorized modifications were made to the Woocommerce Authorize.net payment gateway, with Magecart script injected into the plugin file (www.iottie.com/wp-content/plugins/woocommerce-gateway-authorize-net-cim/assets/js/frontend/wc-authorize-net-cim.min.js).

However, on June 2, 2023, during our client's WordPress/plugin update, the malicious code had already been removed. Nevertheless, upon discovery, on June 13, 2023, iottie's cyber technician thoroughly updated the affected WordPress platform, installed an application-level firewall for enhanced security, established two-factor authentication for all administrator accounts, and changed all passwords.

Our client will be notifying all 241 affected individuals whose credit card information could have been hacked. There were **four (4)** MD residents affected. A copy of the sample notice is attached hereto, and we will wait for your approval to send them via email.

Should you have any questions or concerns, please contact me on my cell at (201) 741-1114.

Very truly yours,
Law Offices of Daniel D. Kim

(Encls.)

Daniel D. Kim
By: Daniel D. Kim, Esq.

LAW OFFICES OF DANIEL D. KIM

Attorneys at Law
416 E. Central Blvd., 2nd Fl.
Palisades Park, NJ 07650

Tel. (201) 947-2188 Fax. (646) 349-1732 E-mail: danielkimlaw@gmail.com

New York Office
5 Penn Plaza, 23rd Fl.,
New York, New York 10001

SAMPLE

NOTICE OF DATA BREACH

Via E-Mail [REDACTED]

Attention: [REDACTED]

Dear Customer:

Our client's business at iottie.com values your business and respects 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 involved your credit card information.

On June 13, 2023, our client discovered through an IT staff that their web store at www.iottie.com had been compromised. Unfortunately, your card information could have been e-skimmed by criminals. We believe criminal e-skimming occurred from April 12, 2023, through June 2, 2023. However, on June 2, 2023, during a WordPress/plugin update, the malicious code was removed. Nevertheless, they could have obtained your credit card information to purchase our client's product online at www.iottie.com. Therefore, we notify you immediately to take the necessary safety measures.

Our client's company, iottie, values your privacy and deeply regrets that this incident occurred. iottie has implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of iottie's valued customers. We also are working closely with fiserv and major credit card law enforcement to ensure the incident is properly addressed.

WHAT YOU CAN DO

Please also review the attachment to this letter for further information on steps you can take to protect your information.

FOR MORE INFORMATION

For further information and assistance, please get in touch with our client's team manager, Julie Ko, at (201) 580-2683 between 10:00 a.m.- 3:00 p.m. Eastern Time.

Very truly yours,

Daniel D. Kim

Daniel D. Kim, Esq.
(201) 741-1114

(Enclosure)

Steps You Can Take to Further Protect Your Information

- **Consider Placing a Fraud Alert on Your Credit Card**

We recommend placing a fraud alert on your credit card.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by closely reviewing your credit card statements. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to [IdentityTheft.gov](https://www.identitytheft.gov) or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.