Clark Hill

Jason Schwent
T (312) 985-5939
Email: jschwent@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

April 14, 2026

VIA PORTAL SUBMISSION

Office of the Attorney General
1125 Washington St SE
Olympia, WA

Dear Attorney General Brown:

We represent Pediatric Products, LLC ("Pediatric Products") with respect to a data security incident involving personal information as described below. Pediatric Products takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

On or around February 17, 2026, Pediatric Products discovered suspicious activity in its network. Pediatric Products immediately implemented its incident response protocols, took the network offline, and engaged external cybersecurity experts to conduct an investigation. The investigation determined that an unauthorized individual gained access to the Pediatric Products network for a limited period of time and may have obtained a limited number of files. Pediatric Products conducted a thorough review of the files at issue and determined that those responsible may have been able to have accessed personal information during the incident.

Impacted information may include names, and some combination of addresses, dates of birth, diagnosis codes, insurance information, and identification numbers.

2. Number of Washington residents affected

Four thousand three hundred residents of Washington were notified of the incident. The cost of providing notification to individuals was above $250,000, and as such, Pediatric Products provided substitute notice via a conspicuous posting on the website on April 10, 2026 and media notice to major nationwide media outlets. A copy of the substitute notice is attached as Exhibit A.

3. Steps taken in response to the incident

In response to the incident, Pediatric Products has changed system and user passwords, restored its systems, and implemented additional endpoint threat detection tools in the network, among other measures.

4. Contact information

Pediatric Products takes the security of the information in its control seriously. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

Jason Schwent
Member

cc: Sunaina Ramesh – sramesh@clarkhill.com

Notice of Data Security Incident

Pediatric Products, LLC ("Pediatric Products") is providing notice to customers of a recent cybersecurity incident via this posting. Pediatric Products learned of this incident when it identified suspicious network activity and immediately took action to secure its environment. There is no evidence that any personal information has been or will be misused as a result of this incident. The security of personal information is very important to us, and we sincerely apologize for any inconvenience this may cause.

What Happened?

On or around February 17, 2026, we discovered suspicious activity in our network. We immediately implemented our incident response protocols, took our network offline, and engaged external cybersecurity experts to conduct an investigation. The investigation determined that an unauthorized individual gained access to the Pediatric Products network for a limited period of time and may have obtained a limited number of files. Pediatric Products conducted a thorough review of the files at issue and determined that those responsible may have been able to have accessed personal information during the incident. Impacted files may have included customers' names, and some combination of the following data elements: addresses, dates of birth, diagnosis codes, insurance information, and identification numbers.

What We Are Doing:

We want to assure you that we are taking steps to minimize the risk of this happening in the future. Since the incident, we have changed system and user passwords, restored our systems, and implemented additional endpoint threat detection tools in our network, among other measures. We have no evidence that any of the information impacted by this incident has been misused, but we wanted to make you aware of this out of an abundance of caution.

What You Can Do:

We encourage you to remain vigilant against incidents of identity theft by reviewing bank accounts and other financial statements. You can also visit the Federal Trade Commission's website for more information on protecting your identity at consumer.ftc.gov/identity-theft-and-online-security.

For More Information:

Individuals should contact cybersecurityincident@xpressnebs.com with any questions. Protecting personal information is of the utmost importance to Pediatric Products, and we sincerely apologize for any concern this incident may cause.

Clark Hill

Jason Schwent
T (312) 985-5939
Email: jschwent@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

April 14, 2026

VIA PORTAL SUBMISSION

Office of the Attorney General
1125 Washington St SE
Olympia, WA

Dear Attorney General Brown:

We represent Pediatric Products, LLC ("Pediatric Products") with respect to a data security incident involving personal information as described below. Pediatric Products takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

On or around February 17, 2026, Pediatric Products discovered suspicious activity in its network. Pediatric Products immediately implemented its incident response protocols, took the network offline, and engaged external cybersecurity experts to conduct an investigation. The investigation determined that an unauthorized individual gained access to the Pediatric Products network for a limited period of time and may have obtained a limited number of files. Pediatric Products conducted a thorough review of the files at issue and determined that those responsible may have been able to have accessed personal information during the incident.

Impacted information may include names, and some combination of addresses, dates of birth, diagnosis codes, insurance information, and identification numbers.

2. Number of Washington residents affected

Four thousand three hundred residents of Washington were notified of the incident. The cost of providing notification to individuals was above $250,000, and as such, Pediatric Products provided substitute notice via a conspicuous posting on the website on April 10, 2026 and media notice to major nationwide media outlets. A copy of the substitute notice is attached as Exhibit A.

3. Steps taken in response to the incident

In response to the incident, Pediatric Products has changed system and user passwords, restored its systems, and implemented additional endpoint threat detection tools in the network, among other measures.

4. Contact information

Pediatric Products takes the security of the information in its control seriously. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

Jason Schwent
Member

cc: Sunaina Ramesh – sramesh@clarkhill.com

Notice of Data Security Incident

Pediatric Products, LLC ("Pediatric Products") is providing notice to customers of a recent cybersecurity incident via this posting. Pediatric Products learned of this incident when it identified suspicious network activity and immediately took action to secure its environment. There is no evidence that any personal information has been or will be misused as a result of this incident. The security of personal information is very important to us, and we sincerely apologize for any inconvenience this may cause.

What Happened?

On or around February 17, 2026, we discovered suspicious activity in our network. We immediately implemented our incident response protocols, took our network offline, and engaged external cybersecurity experts to conduct an investigation. The investigation determined that an unauthorized individual gained access to the Pediatric Products network for a limited period of time and may have obtained a limited number of files. Pediatric Products conducted a thorough review of the files at issue and determined that those responsible may have been able to have accessed personal information during the incident. Impacted files may have included customers' names, and some combination of the following data elements: addresses, dates of birth, diagnosis codes, insurance information, and identification numbers.

What We Are Doing:

We want to assure you that we are taking steps to minimize the risk of this happening in the future. Since the incident, we have changed system and user passwords, restored our systems, and implemented additional endpoint threat detection tools in our network, among other measures. We have no evidence that any of the information impacted by this incident has been misused, but we wanted to make you aware of this out of an abundance of caution.

What You Can Do:

We encourage you to remain vigilant against incidents of identity theft by reviewing bank accounts and other financial statements. You can also visit the Federal Trade Commission's website for more information on protecting your identity at consumer.ftc.gov/identity-theft-and-online-security.

For More Information:

Individuals should contact cybersecurityincident@xpressnebs.com with any questions. Protecting personal information is of the utmost importance to Pediatric Products, and we sincerely apologize for any concern this incident may cause.