

IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY
FIRST JUDICIAL DISTRICT OF PENNSYLVANIA
CIVIL TRIAL DIVISION

Filed and Attested by the
Office of Judicial Records
15 MAR 2022 06:04 pm
S. RICE

COMMONWEALTH OF PENNSYLVANIA :
By Attorney General Josh Shapiro :
 :
Petitioner :
 :
v. :
 :
HANNA ANDERSSON, LLC :
 :
 :
Respondent :

ASSURANCE OF VOLUNTARY COMPLIANCE

The Commonwealth of Pennsylvania by Attorney General Josh Shapiro (“Commonwealth”) and Hanna Andersson, LLC. (“Hanna”) enter into the following Assurance of Voluntary Compliance (“Assurance”) pursuant to the Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, *et seq.*; 201-5 (“Consumer Protection Law”):

1. PREAMBLE

1.1. The Commonwealth conducted an investigation under the Consumer Protection Law regarding the data breach announced by Hanna on January 15, 2020. The breach affected approximately 6,000 Pennsylvania customers from October 7, 2019 and November 11, 2019.

1.2. On December 5, 2019, Hanna received a Common Point-of-Purchase (“CPP”) notification. Moreover, on the same day, law enforcement notified Hanna that approximately 104,000 credit cards traced to Hanna were available for purchase on a dark web site.

1.3. The Commonwealth's investigation found that Hanna engaged in deceptive or unfair business practices by making material misrepresentations in its customer-facing privacy policy concerning the safeguarding of its customers' personal information within its e-commerce platform.

1.4. Specifically, Hanna disseminated, or caused to be disseminated, the following statements on its website during the time of the breach:

The security of your personal information is very important to Hanna, and we have implemented measures to ensure your information is processed confidentially, accurately, and securely. Our website is PCI DSS compliant and uses SSL/TLS (Secure Sockets Layer) technology to encrypt your order information, such as your name, address, and credit card number, during data transmission. We use a third-party payment processor, which is also PCI DSS compliant. . . We follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it.

1.5. According to an independent forensic investigator who performed a forensic analysis on Hanna's cardholder data environment following the breach, Hanna failed to meet six (6) of twelve (12) Payment Card Industry Data Security Standards ("PCI DSS").

1.6. Moreover, the forensic investigator listed six (6) potential causes of the breach and made eight (8) recommendations for remediation, six (6) of which were given a "High" priority ranking.

1.7. The Commonwealth alleges that Hanna failed to employ reasonable measures to detect and prevent unauthorized access to its computer network. Therefore, the Commonwealth alleges that Hanna engaged in unfair and deceptive cybersecurity practices that taken together, unreasonably and unnecessarily exposed Pennsylvania consumers' personal data to unauthorized access and theft.

1.8. The Commonwealth alleges Hanna's conduct constitutes unfair methods of competition and/or unfair or deceptive acts or practices in the conduct of trade or commerce in violation of the Consumer Protection Law, including without limitation, the following:

- (i) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a

person has sponsorship, approval status, affiliation or connection that he does not have as prohibited by Section 201-2(4)(v) of the Consumer Protection Law, 73 P.S. § 201-2(4)(v);

(ii) Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another as prohibited by Section 201-2(4)(vii) of the Consumer Protection Law, 73 P.S. § 201-2(4)(vii); and

(iii) Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding in violation of 73 P.S. §201-2(4)(xxi).

1.9. Under Section 201-5 of the Consumer Protection Law and otherwise, this Assurance will not be considered an admission of wrongdoing for any purpose.

2. PARTIES

2.1. Petitioner is the Commonwealth of Pennsylvania, acting by Attorney General Josh Shapiro. The Attorney General is charged with among other things, enforcement of the Consumer Protection Law.

2.2. Respondent Hanna Andersson, LLC (“Hanna” and together with the Commonwealth, the “Parties”) is a Delaware Foreign Limited Liability Company with its principal place of business located at 608 NE 19th Avenue, Portland, Oregon 97232. Hanna engages in trade and commerce in the Commonwealth of Pennsylvania by selling children’s apparel through its e-commerce website. At the time of the breach, Hanna also had two Pennsylvania store locations.

3. DEFINITIONS

3.1. “Cardholder Data Environment” (“CDE”) means Hanna’s personnel, processes, and technologies that store, process, or transmit Payment Card Information of Consumers. The CDE definition also includes system components or devices that are located within or connected to CDE; or provide security services, facilitate segmentation, or may impact the security of the CDE. This definition is intended to be consistent with the PCI DSS.

3.2. “Compensating Controls” means alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined by the official responsible for the Information Security Program or his or her designee to be impractical to implement at the present time due to legitimate technical or business constraints. Such alternative mechanisms must: (1) meet the intent and rigor of the original stated requirement; (2) provide a similar level of security as the original stated requirement; (3) be up-to-date with current industry accepted security protocols; and (4) be commensurate with the additional risk imposed by not adhering to the original stated requirement. The determination to implement such alternative mechanisms must be accompanied by written documentation demonstrating that a risk analysis was performed indicating the gap between the original security measure and the proposed alternative measure, that the risk was determined to be acceptable. This definition is intended to be consistent with the PCI DSS.

3.3. “Consumer” means any Pennsylvania consumer who initiates a purchase of or purchases goods directly from any Hanna store or e-commerce platform.

3.4. “Effective Date” is the date of filing of this Assurance.

3.5. “Payment Card Information” (“PCI”) means Cardholder Data (“CHD”) and Sensitive Authentication Data (“SAD”) as defined by the PCI DSS.

3.6. “PCI DSS” means the latest version of the Payment Card Industry Data Security Standard published by Payment Card Industry Security Standards Council.

3.7. “Personal Information” means information contained within the CDE of Consumers that is (1) “personal information” as defined under the Breach of Personal Information Notification Act, 73 P.S. § 2302 (enacted December 22, 2005), and (2) Payment Card Information (“PCI”).

3.8. “Service Provider” means a business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity.

This also includes companies that provide services that control or could impact the security of cardholder data.

4. APPLICATION

4.1. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance applies to Hanna, its affiliates, subsidiaries, successors and assigns, and its officers and employees.

4.2. Hanna must comply with the Consumer Protection Law in connection with its collection, use, and maintenance of Personal Information, and must maintain reasonable security policies and procedures designed to safeguard Personal Information from unauthorized use or disclosure.

5. REQUIREMENTS

5.1. Unless otherwise specified herein, the requirements set forth in this Assurance applies to Hanna for a period of seven (7) years from the Effective Date.

6. INFORMATION SECURITY PROGRAM

6.1. Hanna must further develop, implement, and maintain a comprehensive information security program to govern the CDE ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information that Hanna collects, stores, transmits, and/or maintains, and that will, at a minimum include the requirements set forth in this Assurance to the extent appropriate based on Hanna's assessment of relevant risks. A determination regarding the extent to which any such requirements defined in this Assurance are not appropriate must be based on a reasonable assessment of relevant risks and documented by Hanna.

6.2. The Information Security Program must include the following components:

- a. Documented methods and criteria for managing information security risks to cardholder data and Personal Information, including assessment, prioritization, reduction, and

acceptance of risks. Hanna's risk assessment methods and risk assessment criteria must conform to an information security risk assessment method that is provided by information security bodies (e.g., NIST Special Publications 800-30, The Sedona Conference Commentary on a Reasonable Security Test (February 2021), ISO 27005, Duty of Care Risk Analysis Standard ("DoCRA"), or Center for Internet Security Risk Assessment Method ("CIS RAM")) and must include the following:

i. The Information Security Program must design, implement, operate, test, and improve safeguards that reduce identified risks to a reasonable and appropriate level and achieve the control objectives listed below:

- (a) The safeguards must not create a likelihood and impact of harm to Consumers or the public interest such that a remedy is needed.
- (b) The safeguards may not require Hanna to curtail its proper objectives (e.g., profit, growth, reputation, market competitiveness) or the utility of Hanna's services to Consumers.
- (c) The burden imposed on Hanna by the safeguards must be proportionate to the risk the safeguards reduce to Consumers and the public interest.

b. Hanna must conduct comprehensive risk assessments to its CDE or any other network where Hanna stores Personal Information at least annually, and upon changes to its systems that may increase risks to Consumers. Comprehensive assessments must include intentional and unintentional foreseeable threats to Personal Information that could harm consumers. Risk assessments must be conducted by parties that are competent to model threats that are relevant to Hanna and who may capably estimate risks that are created by those threats.

c. Resources: Hanna's allocation of risk-appropriate resources to protect Personal Information that may foreseeably harm Consumers and that sufficiently support Hanna's claims about the effectiveness of its Information Security Program.

d. Designation of Responsible Parties: Hanna's assignment of responsibility for operating the Information Security Program to personnel or Service Providers who have sufficient scope of authority and capability to effectively fulfill that role.

e. Information Security Program Assessment: At least annually, Hanna must review the effectiveness of its Information Security Program and safeguards, and correction of vulnerabilities that may pose inappropriate risks. Hanna must review the Information Security Program and controls with sufficient frequency and detail to provide timely and sufficient resources to address vulnerabilities and risks.

f. Management Engagement: Hanna or Service Provider's issuance of reports to management that reasonably and accurately describe the effectiveness of the implementation and operation of safeguards and the overall effectiveness of the Information Security Program. Hanna may achieve this objective through the issuance of audits and issuance of key risk indicators. Audits must occur on at least an annual basis. Controls will be audited with a frequency that is commensurate to the risk of them changing or failing. Key risk indicators, analysis of the effectiveness of the risk management program, will be provided to executive management on at least a quarterly basis. Key risk indicators must provide executives with information sufficient for them to understand the nature and status of cybersecurity risks, and sufficient for them to determine whether priorities or resources should be adjusted to reduce risks to a reasonable and acceptable level.

g. Third-Party Risks: Hanna's inclusion of third parties (e.g., Service Providers) in the Information Security Program to ensure that risks posed by those third parties are reasonable and appropriate.

6.3. Such Information Security Program must be developed and implemented within One Hundred Eighty (180) days after the Effective Date of this Assurance. Hanna's implementation of the Information Security Program must include development of the plan for implementing risk-based safeguards within Ninety (90) days after the Effective Date of this Assurance, and implementation of the planned safeguards within One Hundred Eighty (180) days after the Effective Date of this Assurance. For any requirements not fully developed and implemented within One Hundred Eighty (180) days after the Effective Date of this Assurance, Hanna must implement interim Compensating Controls to address the identified risks.

6.4. The Hanna Information Security Program must be in writing and contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Hanna's operations; (ii) the nature and scope of Hanna's activities; and (iii) the sensitivity of the Personal Information that Hanna maintains.

6.5. Hanna must retain an employee or service provider to be responsible for overseeing Hanna's information security program with appropriate credentials, background and expertise in information security who will be responsible for overseeing Hanna's implementation and maintenance of the Information Security Program.

6.6. Hanna's Information Security Program must include security awareness training designed to communicate Hanna's commitment to full compliance with the Information Security Program and to ensure that all personnel with key responsibilities for implementation and oversight of the Information Security Program, including the person responsible for overseeing the implementation and maintenance of the program (e.g., CISO), have sufficient knowledge of the

requirements of this Assurance, and the specific knowledge, skills, and abilities to perform their functions in compliance with the Information Security Program. Hanna's training must ensure that system, database, network administrators, and persons with privileged access to the CDE are fully informed of the requirements of the Information Security Program relevant to their functions, which may include password policies, secure data handling, secure storage, transmission and disposal of Personal Information, and best practices to prevent attackers from obtaining credentials and other sensitive data through malicious downloads and other threats identified by Hanna. Hanna must also develop accountability metrics to measure each participant's compliance with training requirements. Within Ninety (90) days of the Effective Date, Hanna must provide training required by this Assurance, and thereafter will provide it to relevant personnel on at least an annual basis.

7. INFORMATION SECURITY SAFEGUARDS

7.1. As part of the Information Security Program, Hanna must implement reasonable security for Personal Information by fulfilling control objectives that would have prevented or detected the breach announced by Hanna on January 15, 2020:

a. Personal Information that may harm the public when compromised must be reasonably separated from people and systems that can foreseeably compromise them, and must be reasonably separated from people, systems, and networks that are configured to be less secure than Hanna's risk acceptance criteria. Hanna may achieve this objective by using network segmentation, or other technical, physical, automated, or logical means.

b. Hanna must store event logs and security logs for a period of time that is sufficient to detect, respond to, and investigate security incidents. Hanna may achieve this objective by estimating their time-to-respond during tests of their incident response plan and setting log repository retention periods accordingly.

c. Hanna must implement and maintain logging and log monitoring policies and procedures designed to collect, manage, and analyze security logs and monitor its CDE to detect, understand, or recover from an attack. Hanna may achieve this objective by using a central log management system and log harvesting, parsing, alerting to be notified of anomalies or suspicious activity.

d. Hanna must detect and respond to suspicious network activity within its network within reasonable means. Hanna may achieve this objective by using log correlation and alerting, intrusion detection and prevention systems (IDS/IPS), threat management systems, or other methods and tools.

e. Hanna must operate or allow to be operated within their environment systems, operating systems, and applications that are continuously serviced and maintained by vendors and Service Providers to keep them secure from foreseeable threats. Hanna may achieve this objective by removing deprecated systems and applications from their environment, or only operating systems and applications that are regularly patched by the developer, vendor, or open source communities.

f. Risks posed by third parties (e.g., Service Providers) that may compromise Personal Information and foreseeably harm Consumers must be reduced and maintained at an appropriate level. Hanna will use means in their control to reduce third party risks reasonably and appropriately, where the third parties cannot reasonably do so. Hanna may achieve this objective by risk evaluating and auditing third parties to determine whether they meet Hanna's acceptable risk definition, or may rely on independent third party auditors or certifications that verify the third party's risk management program meets Hanna's requirements (e.g. PCI DSS when the Service Provider may affect the security of PCI).

8. SETTLEMENT COMPLIANCE ASSESSMENT

8.1. Hanna must obtain an information security compliance assessment and report for the CDE from a third-party professional ("Third-Party Assessor"), using procedures and standards generally accepted in the profession ("Third-Party Assessment"), within one (1) year after the Effective Date of this Assurance. The Third-Party Assessor's report must:

- A. Set forth the specific administrative, technical, and physical safeguards maintained by Hanna;
- B. Explain the extent to which such safeguards are appropriate in light of Hanna's size and complexity, the nature and scope of Hanna's activities, and the PCI information handled by Hanna;
- C. Explain the extent to which the safeguards that have been implemented meet the requirements of the Information Security Program; and
- D. Identify Hanna's Qualified Security Assessor for purposes of PCI DSS validation if Hanna is deemed a Level One Merchant.

8.2. Hanna's Third-Party Assessor must (a) be a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization; and (b) have at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

8.3. Within ninety (90) days of completion of the Third-Party Assessor's report, Hanna must notify the Commonwealth of the completion of the report. If the Commonwealth seeks a copy of the Third Party Assessor's report, the Commonwealth will issue an administrative subpoena, under Section 919 of the Administrative Code of 1929, 71 P.S. § 1, *et seq.*, § 307-3, to direct Hanna to produce and deliver or cause to be delivered a copy of the report.

8.4. The identification of any deficiencies or recommendations for correction in the Third Party Assessor's report will not constitute a violation of this Assurance unless such deficiencies otherwise amount to a violation of the other obligations set forth in this Assurance.

9. MONETARY PAYMENT

9.1. Upon execution of this Assurance, Hanna will pay \$40,000.00 (Forty Thousand dollars and 00/100) to the Commonwealth which will be allocated as follows:

9.2. A civil penalty in the amount of \$10,000.00 (Ten Thousand dollars and 00/100).

9.3. The sum of \$30,000.00 (Thirty Thousand dollars and 00/100) to the Commonwealth in costs to be deposited in an interest-bearing account to be used for future public protection and education purposes.

10. GENERAL PROVISIONS

10.1. The Parties understand and agree that this Assurance will not be construed as an approval or a sanction by the Commonwealth of Hanna's business practices, nor will Hanna represent that this Assurance constitutes an approval or sanction of its business practices. The Parties further understand and agree that any failure by the Commonwealth to take any action in response to any information submitted pursuant to this Assurance will not be construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor will it preclude action thereon at a later date.

10.2. Nothing in this Assurance will be construed as relieving Hanna of the obligation to comply with all state and federal laws, regulations, and rules, nor will any of the provisions of this Assurance be deemed to authorize or require Hanna to engage in any acts or practices prohibited by such laws, regulations, and rules.

10.3. Hanna must deliver a copy of this Assurance to, or otherwise fully apprise, each of its current officers of the rank of executive vice president or above, the executive management officer

having decision-making authority with respect to the subject matter of this Assurance, and each member of its Board of Directors within ninety (90) days of the Effective Date. Hanna must deliver a copy of this Assurance to, or otherwise fully apprise, any new officers of the rank of executive vice president or above, new executive management officer having decision-making authority with respect to the subject matter of this Assurance, and each new member of its Board of Directors, within thirty (30) days from which such person assumes his/her position with Hanna.

10.4. This Assurance may be executed by any number of counterparts and by different signatories on separate counterparts, each of which will constitute an original counterpart thereof and all of which together will constitute one and the same document. One or more counterparts of this Assurance may be delivered by facsimile or electronic transmission with the intent that it or they will constitute an original counterpart thereof.

10.5. This Assurance will not be construed to limit any private course of action. This Assurance may be enforced only by the Parties hereto. Nothing in this Assurance will be construed to create, affect, limit, alter, or assist any private right of action, including without limitation any private right of action that a consumer or other third-party may hold against Hanna.

10.6. The Court of Common Pleas of Philadelphia County, Pennsylvania will maintain jurisdiction over the subject matter of this Assurance and over Hanna for the purpose of enforcing this Assurance.

10.7. If any clause, provision, or section of this Assurance is held to be illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability will not affect any other clause, provision, or section of this Assurance, which will be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or provision had not been contained herein.

10.8. Whenever Hanna provides notice to the Attorney General under this Assurance, that requirement will be satisfied by sending notice to John Abel, Assistant Director for Multistate and

Special Litigation. Any notices sent to Hanna pursuant to this Assurance will be sent to the following addresses: Hanna Andersson, 608 NE 19th Ave. Portland, OR 97232, Attn: Director of Cybersecurity, and Perkins Coie LLP, 1201 Third Avenue, Ste. 4900, Seattle WA, 98101, Attn: Amelia Gerlicher. Any Party may update its address by sending written notice to the other Party. All notices under this Assurance will be provided via electronic and overnight mail.

10.9. Hanna certifies that Bradley M. Bell is authorized by the Hanna to enter into this Assurance on behalf of the Hanna and that his/her signature on this document binds the Hanna to all terms herein.

NOW THEREFORE, Hanna agrees by the signing of this Assurance that Hanna must abide by each and every one of the aforementioned terms of this Assurance, and that the Commonwealth may enforce this Assurance pursuant to §201-8 of the Consumer Protection Law by petitioning this Court or any other Court of competent jurisdiction, to order any equitable or other relief which may be deemed necessary and appropriate as provided herein and by law.

FOR THE PETITIONER:

COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ATTORNEY GENERAL

JOSH SHAPIRO
ATTORNEY GENERAL

Date: 3-15-22

By: Tim R. Murphy

TIMOTHY R. MURPHY

Senior Deputy Attorney General

PA Attorney I.D. No. 321294

Bureau of Consumer Protection

1600 Arch Street, Suite 300

Philadelphia, Pennsylvania 19103

Telephone: (215) 560-2414

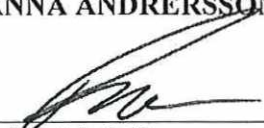
Facsimile: (215) 560-2494

FOR THE RESPONDENT:

HANNA ANDRERSSON, LLC

Date: 3/14/2022

By: _____


Bradley M. Bell
Chief Financial Officer and Chief Operating Officer
608 NE 19th Avenue
Portland, Oregon 97232

Counsel to Hanna

Date: _____

By: _____

Nicholas H. Pennington
PA Attorney I.D. No. 307073
Stevens & Lee P.C.
620 Freedom Business Center, Suite 200
King of Prussia, PA 19406

Amelia M. Gerlicher
Todd M. Hinnen
Perkins Coie LLP
1201 Third Avenue
Suite 4900
Seattle, Washington 98101-3099

FOR THE RESPONDENT:

HANNA ANDRERSSON, LLC

Date: _____

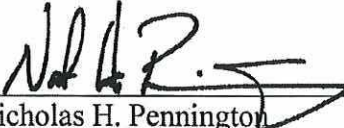
By: _____

Bradley M. Bell
Chief Financial Officer and Chief Operating Officer
608 NE 19th Avenue
Portland, Oregon 97232

Counsel to Hanna

Date: Mar. 14, 2022

By: _____


Nicholas H. Pennington
PA Attorney I.D. No. 307073
Stevens & Lee P.C.
620 Freedom Business Center, Suite 200
King of Prussia, PA 19406

Amelia M. Gerlicher
Todd M. Hinnen
Perkins Coie LLP
1201 Third Avenue
Suite 4900
Seattle, Washington 98101-3099

**IN THE COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY
FIRST JUDICIAL DISTRICT OF PENNSYLVANIA
CIVIL TRIAL DIVISION**


COMMONWEALTH OF PENNSYLVANIA	:
By Attorney General Josh Shapiro	:
	:
Petitioner	:
	:
v.	:
	:
HANNA ANDERSSON, LLC	:
	:
Respondent	:

CERTIFICATE OF SERVICE

I, Timothy R. Murphy, hereby certify that on the date stated below, a true and correct copy of the executed Assurance of Voluntary Compliance was served upon Respondent Hanna Andersson, LLC by serving Respondent's attorney at the following email address:

Amelia Morrow Gerlicher—agerlicher@perkinscoie.com

Date: 3-15-22

By: 
TIMOTHY R. MURPHY
Senior Deputy Attorney General
Attorney I.D. #321294
Commonwealth of Pennsylvania
Office of Attorney General
Bureau of Consumer Protection
1600 Arch Street, 3rd Floor
Philadelphia, PA 19103
215-560-2414
Attorney for Petitioner