RECEIVED
ATTORNEY GENERAL OF OHIO

OCT 25 2022

CONSUMER PROTECTION SECTION
PUBLIC INSPECTION FILE

STATE OF OHIO
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION SECTION

IN THE MATTER OF	)	
	)	DOCKET NO. 598326
AMERICAN FRAME CORPORATION	)	
400 Tomahawk Dr.	)	
Maumee, Ohio 43537	)	

ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance (hereafter "Assurance") is entered into this 25th day of October 2022 by American Frame Corporation and Ohio Attorney General Dave Yost (collectively the "Parties"). For purposes of this Assurance, "Supplier" shall mean American Frame Corporation and its officers, partners, agents, representatives, employees, successors, or assigns and all persons acting in concert or participation with them, directly or indirectly, through any corporate device, partnership, association, or affiliation.

WHEREAS, the Attorney General has investigated Supplier's business practices pursuant to the authority granted the Attorney General by R.C. 1345.06 of the Consumer Sales Practices Act ("CSPA"), R.C. 1345.01 et seq., and by R.C. 1349.191 of the Security Breach Notification Act, R.C. 1349.19 et seq.;

WHEREAS, the Attorney General's investigation has found that Supplier violated R.C. 1349.19(B)(2) of the Security Breach Notification Act;

WHEREAS, American Frame has represented that it has rebuilt and upgraded its entire tech infrastructure and all related systems, including third-party providers and partners;

WHEREAS, R.C. 1345.06(F) of the CSPA grants the Attorney General the authority to enter into and accept an Assurance;

WHEREAS, this Assurance is a promise in writing by Supplier of its intent to conduct its

business in a manner designed to comply with all provisions of the CSPA, R.C. 1345.01 et seq., and the Security Breach Notification Act, R.C. 1349.19 et seq.; and

WHEREAS, Supplier, desiring to comply with all aspects of the CSPA and the Security Breach Notification Act, hereby voluntarily enters into this Assurance with the Attorney General.

NOW THEREFORE, in consideration of the mutual promises and conditions set forth herein, the Parties hereto **AGREE** as follows:

(1) The "Effective Date" shall mean the date that is indicated on the first page of this Assurance.

(2) By accepting this written Assurance, the Attorney General agrees to terminate the current investigation, being conducted by the Attorney General's Consumer Protection Section, of Supplier's business practices and actions occurring on or before the Effective Date of this Assurance.

(3) By giving this written Assurance, Supplier agrees to comply with all the terms of this Assurance and to conduct its business in compliance with all applicable Ohio laws, including without limitation, the CSPA and the Security Breach Notification Act.

BACKGROUND AND STATEMENT OF FACTS

1. Supplier is an Ohio corporation whose principal place of business is located at 400 Tomahawk Drive, Maumee, Ohio 43537.
2. Supplier sells framing and printing related goods and services to consumers nationwide, including via its website www.americanframe.com.
3. Supplier maintains a computer system that contains computerized data that includes Personal Information of its employees and customers. For purposes of this Assurance, "Personal Information" shall have the same definition as in R.C. 1349.19(A)(7).

4. Supplier's website, www.americanframe.com, allows consumers to select items and services to purchase and then pay for the items. Via the professional-looking website, consumers can customize their framing projects, order the customized projects, and pay for them using a payment card.

5. Taken as a whole, the visual design and functionality of the website leads consumers to believe that American Frame is a sophisticated company that utilizes best practices related to appropriate information security practices.

6. Due to the sophistication of Supplier's website and the scale of Supplier's business, Supplier implicitly represented to consumers that their payment information would be maintained in a secure manner during and after the transaction.

7. Post-transaction, Supplier failed to maintain its customers' payment information in a secure manner.

8. On or about August 1, 2020, upon receipt of a ransom note from an unauthorized third-party Threat Actor, Supplier determined it had been the subject of a data cybersecurity attack.

9. The cybersecurity attack resulted in a breach of the security of American Frame's computer system.

10. Initial forensics determined that between the dates of April 23, 2020 and August 2, 2020, the Threat Actor had full access to American Frame's computer system and had access to unencrypted information including, but not limited to, employees' Social Security numbers and customers' credit card numbers, along with the corresponding access codes ("Data Breach").

11. Supplier retained a third-party incident response firm to conduct a forensic investigation regarding the Data Breach. The forensic investigation determined that the root cause of the

breach was the result of access to an administrator account through which the Threat Actor was able to perpetrate the Data Breach due to weaknesses in Supplier's computer system including, but not limited to, the following:

a. Supplier failed to implement a multifactor authentication system, which enabled the Threat Actor to enter Supplier's system by guessing an administrator's password. This allowed the Threat Actor to access Supplier's entire system, including customers' credit card numbers and Human Resources files containing employees' social security numbers;

b. Although Supplier encrypted customers' credit card numbers, Supplier stored the encryption keys for encrypted credit card numbers in plain text in a non-password-protected document, which enabled the Threat Actor to easily access the credit card numbers;

c. Supplier retained old credit card data from customers after it was no longer needed, which enabled the Threat Actor to therefore access more consumers' credit card numbers; and

d. Supplier failed to deploy software security vulnerability patches within 30 days of release.

12. As a result of the weaknesses in Supplier's computer system, the Data Breach resulted in the Personal Information, including full names, addresses, and social security numbers and/or credit card information, including access codes, of Supplier's customers and employees being accessed and/or acquired by the Threat Actor.

13. The Threat Actor's access and/or acquisition of Supplier's customers' and employees' Personal Information put them at risk of identity theft or other fraud.

14. On or about January 14, 2021, Supplier mailed letters notifying affected individuals about the Data Breach. For purposes of this Assurance, "Affected Individuals" shall mean the persons, including American Frame employees and American Frame customers, whose Personal Information was impacted by the Data Breach.

15. Supplier violated R.C. 1349.19(B)(2) of the Security Breach Notification Act, by failing to disclose the Data Breach to the Affected Individuals within 45 days after it had discovered the Data Breach.

COMPLIANCE PROVISIONS

16. Supplier shall not violate the Security Breach Notification Act, R.C. 1349.19 et seq., including, but not limited to, violating the specific provisions described herein.

17. Supplier shall develop and implement an Information Security Program that Supplier shall document in writing. The Information Security Program shall contain administrative, technical, and physical safeguards appropriate to the size and complexity of Supplier's operations, the nature and scope of Supplier's activities, and the sensitivity of the Personal Information that Supplier maintains. At a minimum, Supplier's Information Security Program shall include the establishment of policies and procedures to implement the following:

    a. Regular review and identification of internal and external risks to the security, confidentiality, or integrity of Personal Information of employees and customers that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or any other compromise of such information, and an assessment of the sufficiency of any safeguards in place to control these risks;

    b. The design and implementation of reasonable safeguards to control those risks including, but not limited to, patch management and password management

policies;

c. Regular testing and monitoring of the effectiveness of those safeguards;

d. The evaluation and adjustment of the Information Security Program in light of the results of the testing and monitoring; and

e. Ongoing training of employees and temporary and contract workers regarding the proper handling and protection of Personal Information of employees and customers, the safeguarding of passwords and security credentials for the purpose of preventing unauthorized access to Personal Information, and disciplinary measures for the violation of the Information Security Program.

18. In furtherance of Supplier's Information Security Program, Supplier shall implement and maintain the following business processes:

a. Supplier shall maintain a multi-factor authentication system, or a similarly secure system, for its computer network and any network on which Supplier operates.

b. Within thirty days of the Effective Date of this Assurance, Supplier shall implement and maintain a process to segment all Personal Information, including customers' payment card information and employees' Social Security numbers, from the rest of its computer system.

c. Within thirty days of the Effective Date of this Assurance, Supplier shall implement and maintain a process to encrypt all Personal Information of employees and customers on Supplier's network environment, whether the information is in transit through Supplier's system or at rest. "Network environment" is defined as the servers, both physical and virtual, and workstations controlled and maintained by Supplier. In the event that Supplier does not maintain Personal Information of

employees and/or customers within its own network environment, Supplier shall ensure that the business(es) to whom this information is entrusted for processing and/or storage implements and maintains a process to encrypt all Personal Information of employees and customers.

d. Within thirty days of the Effective Date of this Assurance, Supplier shall implement and maintain a process to securely discard customers' payment card information, as soon as reasonably practicable after the information is no longer needed. In the event that Supplier does not maintain customers' payment card information within its own network environment, Supplier shall ensure that the business(es) to whom this information is entrusted for processing and/or storage implements and maintains a process to securely discard customers' payment card information, as soon as reasonably practicable after the information is no longer needed.

e. Within thirty days of the Effective Date of this Assurance, Supplier shall implement and maintain a process to discard former employees' Social Security Numbers and any other Personal Information, as soon as reasonably practicable, after the Personal Information is no longer needed.

f. Supplier shall implement and maintain an appropriate system to collect and monitor network activity, such as through the use of a security information and event management tool. Supplier shall implement appropriate policies and procedures to ensure that such a tool is properly configured to report anomalous activity.

g. Supplier shall maintain and keep up-to-date all software associated with its maintenance and safeguarding of Personal Information or maintain appropriate compensating controls to safeguard the confidentiality and integrity of such

Personal Information.

h. Supplier shall implement appropriate steps designed to reasonably manage the review of industry-accepted payment card security technologies relevant to Supplier's business. Where appropriate and reasonable, Supplier shall adopt any such improvements.

i. Supplier shall devalue payment card information, including, but not limited to, encryption and/or tokenization, to obfuscate payment card information throughout the course of retail transactions with Supplier. In the event that Supplier does not maintain customers' payment card information within its own network environment, Supplier shall ensure that the business(es) to whom this information is entrusted for processing and/or storage implements and maintains a process to devalue payment card.

19. Supplier may satisfy the implementation and maintenance of the Information Security Program and the safeguards required by this Assurance through review, maintenance, and, if necessary, updating, of an existing information security program or existing safeguards, provided that such existing information security program and existing safeguards meet the requirements set forth in this Assurance.

20. Supplier shall at all times retain an employee or a third-party consultant with appropriate background or experience in information security who shall be responsible for implementing and maintaining the Information Security Program. This individual shall also be responsible for advising Supplier's management of Supplier's security posture, security risks faced by Supplier, and security implications of Supplier's decisions.

21. Supplier shall ensure that its Information Security Program receives the resources and support

reasonably necessary to ensure that the Information Security Program functions as intended by this Assurance.

22. Supplier must regularly test or monitor the effectiveness of the Information Security Program implemented in accordance with this Assurance.

23. Supplier shall retain a qualified third-party auditor with expertise in information systems security to conduct an audit of Supplier's Information Security Program. The audit shall commence no sooner than one year but no later than fourteen months after the Effective Date of this Assurance. Within eighteen months after the Effective Date of this Assurance, the third-party auditor shall submit the audit report required by this Paragraph to the Attorney General. The audit of Supplier's Information Security Program shall, at a minimum, specifically address Supplier's compliance with the requirements set forth in Paragraphs 17 and 18 of this Assurance.

24. Supplier shall comply with the reporting and notification requirements of R.C. 1349.19. Further, for a period of five years following the Effective Date of this Assurance, if Supplier experiences a future Security Incident in which Personal Information has been accessed, Supplier must notify the Attorney General about the incident within thirty calendar days of Supplier's discovery of the Security Incident. For purposes of this Assurance, "Security Incident" shall refer to any compromise or threat that gives rise to a reasonable likelihood of compromise, by unauthorized access or inadvertent disclosure, impacting the confidentiality, integrity, or availability of an individual's Personal Information held or stored by Supplier, including but not limited to a data breach.

25. Supplier shall resolve in good faith all future complaints filed by consumers with the Attorney General's Office about any conduct of Supplier that occurs after the Effective Date of this

Assurance.

GENERAL PROVISIONS

26. By accepting this written Assurance, the Attorney General agrees to terminate the current investigation into Supplier's business practices occurring prior to the date of this Assurance.
27. Supplier understands and agrees that this Assurance applies to any related owners, principals, officers, directors, agents, representatives, salespersons, employees, instructors, independent contractors, successors and assigns.
28. This Assurance shall be governed by laws of the State of Ohio.
29. This Assurance is entered into by Supplier of its own free and voluntary act, and with full knowledge and understanding of the nature of the proceedings and the obligations and duties imposed by this Assurance.
30. This Assurance does not constitute an approval by the Attorney General of any of Supplier's business practices, and Supplier shall not represent directly or indirectly, or in any way whatsoever, that the Attorney General has sanctioned, condoned, or approved any part or aspect of its business practices.
31. This Assurance sets forth the entire agreement between the Attorney General and Supplier and supersedes any and all prior agreements or understandings, whether written or oral, between the Parties and/or their respective counsel regarding the subject matter hereof. This Assurance may be amended by written agreement of the Parties, subject to any further requirements under state law.
32. The Parties hereto acknowledge that no other promises, representations, or agreements of any nature have been made or entered into by the Parties. The Parties further acknowledge that

this Assurance constitutes a single and entire agreement that is not severable or divisible, except that if any provision herein is found to be legally insufficient or unenforceable, the remaining provisions shall continue in full force and effect.

33. This Assurance is a public record and shall be filed in the Attorney General's Public Inspection File pursuant to R.C. 1345.05(A)(3).

RELIEF FOR AFFECTED INDIVIDUALS

34. Supplier shall offer extended credit monitoring and identity theft protection services to all Affected Individuals who are residents of Ohio and any other Affected Individuals who are either current or former employees but who do not reside in Ohio ("Ohio Affected Individuals"). Supplier shall provide notification of the offer of extended credit monitoring and identity theft services to the Ohio Affected Individuals in the following manner:

    a. Supplier shall issue direct notification via Regular U.S. Mail or direct electronic mail to all Ohio Affected Individuals within thirty days of the Effective Date of this Assurance.

    b. The deadline for Ohio Affected Consumers to enroll in extended credit monitoring and identity theft protection services shall be no less than 90 days after Supplier issues the notice. The extended credit monitoring shall last for a term of no less than one year from the date on which the consumer enrolls.

PAYMENT TO THE STATE

35. As part of the consideration for the termination of this investigation, Supplier shall make a payment to the State of Ohio in the amount of $60,000. The payment shall be placed in the Attorney General's Consumer Protection Enforcement Fund, to be used by the Attorney General as provided by R.C. 1345.51.

36. The payment required by Paragraph 35 shall be due upon the execution of this Assurance and shall be made by delivering a certified check or money order, containing the code "CPS" in the memo line and payable to the "Ohio Attorney General's Office," to:

Consumer Protection Section
Ohio Attorney General's Office
Attn: Finance Specialist
30 E. Broad Street, 14th Floor
Columbus, Ohio 43215

PENALTIES FOR FAILURE TO COMPLY

37. The Attorney General may assert any claim that Supplier has violated this Assurance in a separate civil action to enforce the terms of this Assurance against Supplier, and the Court shall apply applicable standards of law to determine damages for any subsequent violations, which may include any and all remedies available to the Attorney General pursuant to R.C. 1345.07.

38. Pursuant to R.C. 1345.06(F), this Assurance is not, and shall not be construed as, evidence of any violation of the CSPA and its Substantive Rules by Supplier. Evidence of a violation of an Assurance of Voluntary Compliance, though, is prima-facie evidence of an act or practice in violation of the CSPA, R.C. 1345.01 et seq., if presented after the violation in an action brought under the CSPA, R.C. 1345.01 et seq.

39. This Assurance shall in no way exempt Supplier from any other obligation imposed by law, and nothing contained herein shall relieve Supplier of any legal responsibility for any acts or practices it has engaged in other than those specifically addressed by this Assurance.

40. Nothing in this Assurance shall in any way preclude any investigative or enforcement action(s) against Supplier under any legal authority granted to the Ohio Attorney General:

    a. With respect to the transactions that are the subject of this enforcement action if the terms of the Assurance are not fully obeyed; or,

b. With respect to transactions or occurrences that are not the subject of this Assurance.

WHEREFORE, the parties hereto affix their signatures in recognition and acceptance of the terms contained herein and warrant and represent that by affixing their signatures below they have the legal right to do so.

SIGNATURES

Accepted:

DAVE YOST
ATTORNEY GENERAL

By: _____ Date: 10/25/22

Tracy Morrison Dickens
Senior Assistant Attorney General
Consumer Protection Section
30 E. Broad Street, 14th Floor
Columbus, Ohio 43215
(614) 466-3999
Tracy.Dickens@OhioAGO.gov
Counsel for the Ohio Attorney General

Accepted:

AMERICAN FRAME CORPORATION

By: _____ Date: Oct 17, 2022

Laura Jajko, President
American Frame Corporation
400 Tomahawk Dr.
Maumee Ohio 43537

Accepted:

Mark Wagoner, Esq.

By: _____ Date: 10/17/22

Mark Wagoner
Shumaker, Loop & Kendrick, LLP
1000 Jackson Street
Toledo, Ohio 43604
(419) 321-1412
mwagoner@shumaker.com
Counsel for American Frame Corporation