

**IN THE COURT OF COMMON PLEAS OF  
YORK COUNTY, PENNSYLVANIA**

**COMMONWEALTH OF PENNSYLVANIA** :  
**By Attorney General Michelle A. Henry** :  
 :  
 :  
 **Petitioner** :  
 **v.** :  
 :  
 **CHR Corp. d/b/a Rutter's** :  
 :  
 :  
 **Respondent** :

**ASSURANCE OF VOLUNTARY COMPLIANCE**

The Commonwealth of Pennsylvania by Attorney General Michelle A. Henry (“Commonwealth”) and CHR Corp. d/b/a Rutter’s (“Rutter’s”) enter into an 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”) to resolve the investigation into the data security incident announced by Rutter’s on or about February 13, 2020.

**SUMMARY OF THE INVESTIGATION**

1. The Commonwealth contends that: (1) Rutter’s failed to use appropriate information security practices to protect its customers’ payment card information; and (2) as a result a hacker was able to obtain information related to at least 1,365,995 payment cards used over the course of 272 days at 79 store locations.

2. Rutter’s is a privately held company, headquartered and incorporated in the Commonwealth of Pennsylvania, and engages in trade or commerce by owning and operating a chain of convenience stores and fuel stations throughout the Commonwealth of Pennsylvania.

3. In connection with the sale of its goods and services, Rutter's stores, processes, transmits, and receives payment card information ("PCI") from customers to and from credit card brands.

4. On May 28, 2019, Rutter's first became aware of unauthorized activity on its network when the company received two endpoint security solution alerts, which detailed the execution of suspicious PowerShell scripts and unauthorized lateral movement using compromised credentials of Rutter's employees. Rutter's implemented measures that stopped the unauthorized access by May 29, 2019.

5. Upon receipt of the alerts, the company began an internal investigation and confirmed that malicious PowerShell scripts had been run against certain Rutter's store locations. A cybersecurity firm was engaged to conduct an investigation to determine the cause of the attack and whether PCI was exfiltrated from the network. The cybersecurity firm observed RAM scraping malware but concluded that the threat actors did not successfully exfiltrate cardholder data.

6. In December 2019, Rutter's was notified by its payment processor, Fiserv, that Mastercard identified a pattern of unauthorized charges associated with thirty Rutter's store locations. As a result, Mastercard required Rutter's to engage a PCI Forensic Investigator ("PFI") to perform an investigation of the cardholder data environment.

7. On January 14, 2020, the PFI discovered forensic evidence, not located during the prior investigation, which indicated that the threat actors were able to exfiltrate PCI. Moreover, the PFI found that Rutter's was not compliant with certain provisions of the Payment Card Industry Data Security Standards ("PCI DSS").

8. The Commonwealth's investigation found shortcomings in Rutter's data security, including the following:

- a. Non-compliance with the PCI DSS;

- b. Legacy Service Accounts with weak passwords running on the network;
- c. Identified risks that were consistently not remediated by the company; and
- d. Retention of log data.

9. The Commonwealth alleges that Rutter's failure to employ reasonable security measures to protect consumers' personal information constitute unfair or deceptive acts or practices in violation of the Consumer Protection Law.

10. Under Section 201-5 of the Consumer Protection Law and otherwise, this Assurance will not be considered an admission of wrongdoing for any purpose. For the purposes of this Assurance, Rutter's neither admits nor denies any of the findings in this Section.

#### PARTIES

11. Petitioner is the Commonwealth of Pennsylvania, acting by Attorney General Michelle A. Henry. The Attorney General is charged with among other things, enforcement of the Consumer Protection Law.

12. Respondent CHR Corp. d/b/a Rutter's ("Rutter's" and together with the Commonwealth, the "Parties") is a Pennsylvania corporation that is headquartered in York, PA.

#### ASSURANCES

13. For the purposes of this Assurance, the following definitions will apply:

a. **"Cardholder Data"** means the cardholder name, primary account number (PAN), expiration date, service code, and any associated sensitive authentication data. If the PAN or sensitive authentication data are not present, the data is not Cardholder Data.

b. **"Cardholder Data Environment"** ("CDE") means Rutter's personnel, processes, and technologies that store, process, or transmit Cardholder Data of Consumers. The CDE definition also includes system components or devices that are located within or have unrestricted connections to CDE, and components, people and processes that could



impact the security of the CDE. This definition is intended to be consistent with guidance in the PCI DSS regarding the scope of the CDE.

c. **“Compensating Controls”** means the definition of Compensating Controls found in PCI DSS Appendix B. The determination to implement a Compensating Controls must be documented and indicate that the CISO or his or her designee agrees with the determination.

d. **“Consumer”** means any person who initiates a purchase of or purchases goods directly from any Rutter’s Pennsylvania store location.

e. **“Effective Date”** means date of filing.

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

g. **“Payment Card Industry Data Security Standard”** (“PCI DSS”) means the active and applicable version of the Payment Card Industry Data Security Standard published by the Payment Card Industry Security Standards Council.

h. **“Sensitive Personal Information”** means information contained within the CDE of Consumers that is PCI and “personal information” of Consumers as defined under the Breach of Personal Information Notification Act, 73 P.S. § 2302.

#### **APPLICATION**

14. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance apply to Rutter’s, its affiliates, subsidiaries, successors, and assigns, and its officers and employees in the scope of the performance of their job duties for Rutter’s for a period of five (5) years from the Effective Date.

#### **GENERAL COMPLIANCE**

15. Rutter's must comply with the Consumer Protection Law in connection with its collection, use, and maintenance of Sensitive Personal Information, and must maintain reasonable security policies and procedures designed to safeguard Sensitive Personal Information from unauthorized access or disclosure.

16. Rutter's must comply with the Breach of Personal Information Notification Act ("BPINA"), 73 P.S. § 2301 *et seq.*

### **INFORMATION SECURITY PROGRAM**

17. Rutter's must further develop, implement, and maintain a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Sensitive Personal Information that Rutter's 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 Rutter'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 Rutter's.

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

a. Documented methods and criteria for managing information security risks to Sensitive Personal Information, including assessment, prioritization, reduction, and acceptance of risks. Rutter's risk assessment and risk assessment criteria must use a 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") Version 2.0).

b. The Information Security Program must design, implement, operate, test, and improve safeguards that reduce identified risks to a reasonable and appropriate level that balances all three of these factors:

- i. The safeguards reduce the risk based on a consideration of the interests (e.g., potential harm) of Rutter's and Consumers that may be affected by the risk.
- ii. The safeguards may not require Rutter's to curtail its proper objectives (e.g., profit, growth, reputation, market competitiveness) or the utility of Rutter's services to Consumers.
- iii. The burden imposed on Rutter's by the safeguards must be proportionate to the risk the safeguards reduce to Consumers and the public interest.

c. Rutter's must conduct comprehensive risk assessments, inclusive of the CDE and any network where Rutter's stores Sensitive Personal Information, at least annually. Within a reasonable period of time after changes to the security of its CDE or any other network where Rutter's stores Sensitive Personal Information that may significantly increase risks to Consumers, Rutter's will assess the impact of the change. Comprehensive assessments must include intentional and unintentional foreseeable threats to Sensitive Personal Information that could harm Consumers. Risk assessments must be conducted by parties that are competent to model threats that are relevant to Rutter's and who may capably estimate risks that are created by those threats.

d. At least annually, Rutter's must review the effectiveness of its Information Security Program.

19. Such Information Security Program must be developed and implemented within One Hundred Eighty (180) days after the Effective Date of this Assurance. Failure to fully develop or implement such requirements within One Hundred Eighty (180) days after the Effective Date will not



constitute a violation of this Assurance so long as Rutter's implements interim risk reduction measures to address the identified risks until such requirements are fully developed and implemented.

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

21. Rutter's must designate a qualified individual or service provider with appropriate credentials, background and expertise in information security who will be responsible for overseeing Rutter's implementation and maintenance of the Information Security Program. The duties and responsibilities of the qualified individual or Service Provider must be documented and include advising senior leadership, which may include the Chief Executive Officer and the Board of Directors, of Rutter's security posture, security risks, and security remediation.

22. Rutter's Information Security Program must include security awareness training to all personnel with key responsibilities for implementation and oversight of the Information Security Program. Rutter's training must ensure that its systems, databases, network administrators, and persons with privileged access to Sensitive Personal Information 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 Sensitive Personal Information, and reasonable practices to prevent attackers from obtaining credentials and other sensitive data through malicious downloads and other threats identified by Rutter's. Within Ninety (90) days of the Effective Date, Rutter's must provide training required by this Assurance, and thereafter will provide it to relevant personnel on at least an annual basis.

#### **INFORMATION SECURITY SAFEGUARDS**

23. Rutter's must comply with PCI DSS with respect to its CDE.

24. As part of the Information Security Program, Rutter's must implement reasonable security measures for Sensitive Personal Information including, but not limited to, the following control objectives:

a. Sensitive Personal Information must be transmitted and stored so that it is accessible only to people and systems that need the information for a legitimate business purpose. Rutter's may achieve this objective through access controls or by encrypting, tokenizing, or de-identifying Sensitive Personal Information.

b. Rutter's must disable and/or remove any service accounts that are no longer used for any legitimate business purpose performed on the Rutter's network.

c. Rutter's must implement appropriate password management practices.

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

e. Rutter's must use appropriate authentication measures to verify that people and systems that use credentials are who they purport to be by using technical, physical, or procedural mechanisms that are commensurate with the risk posed by abusing access to Sensitive Personal Information. Rutter's may achieve this objective by providing multi-factor authentication, one-time passcodes, location-specific requirements, or other control enhancements.

f. Rutter's must implement and maintain logging and log monitoring policies and procedures designed to collect, manage, and analyze security logs and monitor where Rutter's stores Sensitive Personal Information to detect, understand, or recover from an attack. Rutter's



may achieve this objective by using a central log management system and log harvesting, parsing, alerting to be notified of anomalies or suspicious activity.

g. Rutter's must store event logs and security logs for a period of time that is sufficient to detect, respond to, and investigate security incidents. Rutter's may achieve this objective by estimating their time-to-respond during tests of their incident response plan and setting log repository retention periods accordingly or by using readily available information regarding the length of time to detect security incidents.

h. Rutter's must maintain, keep updated, and support the software on its network, taking into consideration the impact a software update will have on data security in the context of its network and its ongoing business and network operations, and the scope of the resources required to maintain, update, and support the software. For any software that will no longer be supported by its manufacturer or a third party, Rutter's must commence the evaluation and planning to replace the software or to maintain the software with appropriate Compensating Controls to address the identified risks within a reasonable time period from the date the manufacturer or third party announces that it is no longer supporting the software.

i. Rutter's must detect and respond to suspicious network activity within its network using reasonable means. Rutter's may achieve this objective by using log correlation and alerting, file integrity monitoring, data integrity monitoring, security information and event management systems, intrusion detection and prevention systems, threat management systems, and other methods and tools.

#### **SETTLEMENT COMPLIANCE ASSESSMENT**

25. Rutter's 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 Rutter’s;
- b. Explain the extent to which such safeguards are appropriate in light of Rutter’s size and complexity, the nature and scope of Rutter’s activities, and the Sensitive Personal Information that is handled by Rutter’s;
- c. Explain the extent to which the safeguards that have been implemented meet the requirements of the Information Security Program.
- d. A report on compliance (ROC) from a qualified security assessor (QSA) for purposes of PCI DSS validation will satisfy this Third-Party Assessment requirement.

26. Rutter’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.

27. Within ninety (90) days of completion of the Third-Party Assessor’s report, Rutter’s 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 Rutter’s to produce and deliver or cause to be delivered a copy of the report.

28. 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.

### **PAYMENT TO COMMONWEALTH**

29. Rutter's will pay or cause to be paid \$1,000,000.00 (One Million Dollars and 00/100) to the Commonwealth. Payment must be made no later than thirty (30) days after the Effective Date of this Assurance and the receipt of such payment instructions by Rutter's from the Commonwealth.

### **RELEASE**

30. Following full payment, the Commonwealth will hereby release and discharge Rutter's from all civil claims that the Commonwealth could have brought under the Consumer Protection Law, BPINA, or any other common law claims based on Rutter's alleged conduct related to the data security incident announced on February 13, 2020. Nothing contained in this paragraph will be construed to limit the ability of the Attorney General to enforce the obligations that Rutter's has under this Assurance. Further, nothing in this Assurance will be construed to create, waive, or limit any private right of action.

### **GENERAL PROVISIONS**

31. The Parties understand and agree that this Assurance will not be construed as an approval or a sanction by the Commonwealth of Rutter's business practices, nor will Rutter's 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.

32. Nothing in this Assurance will be construed as relieving Rutter's 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 Rutter's to engage in any acts or practices prohibited by such laws, regulations, and rules.



33. Nothing in this Assurance is intended to constitute an admission or waiver by Rutter's.

34. Rutter's must deliver a copy of this Assurance to, or otherwise fully apprise, each of its current corporate officers having decision-making authority with respect to this Assurance, and each member of its Board of Directors within ninety (90) days of the Effective Date. Rutter's must deliver a copy of this Assurance to, or otherwise fully apprise, any new officers having decision-making authority with respect to this Assurance, and each new member of its Board of Directors, within thirty (30) days from which such person assumes his/her position with Rutter's.

35. 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 electronic transmission with the intent that it or they will constitute an original counterpart thereof.

36. This Court will maintain jurisdiction over the subject matter of this Assurance and over Rutter's for the purpose of enforcing this Assurance. Rutter's agrees to pay all court costs associated with the filing of this Assurance. No court costs, if any, will be taxed against the Commonwealth.

37. 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.

38. Whenever Rutter's provides notice to the Attorney General under this Assurance, that requirement will be satisfied by sending notice to the Assistant Director for Cybersecurity and Technology, Strawberry Square, 15<sup>th</sup> Floor, Harrisburg, PA 17120. Any notices sent to Rutter's pursuant to this Assurance will be sent to the following addresses: CHR Corp., 2295 Susquehanna

Trail, Suite C, York, PA 17404, Attn: Chris Reed and BakerHostetler LLP, 312 Walnut Street, Suite 3200, Cincinnati, OH 45202, Attn: Craig Hoffman | Joseph Bruemmer. Any Party may update its address by sending written notice to the other Party. All notices under this Assurance will be provided via overnight mail and by electronic mail if an email address has been provided for notice.

39. Rutter's certifies that Scott Hartman, President and CEO, is authorized by Rutter's to enter into this Assurance on behalf of Rutter's and that his/her signature on this document binds Rutter's to all terms herein.

**NOW THEREFORE**, Rutter's agrees by signing this Assurance, Rutter's 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, 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

MICHELLE A. HENRY  
ATTORNEY GENERAL

Date: 10/10/23

By: 


**TIMOTHY R. MURPHY**  
*Senior Deputy Attorney General*  
PA Attorney I.D. No. 321294  
**DEBRA DJUPMAN WARRING**  
*Senior Deputy Attorney General*  
PA Attorney I.D. 206437  
Office of Attorney General  
1600 Arch Street, Suite 300  
Philadelphia, Pennsylvania 19103  
Telephone: (215) 560-2414  
Facsimile: (215) 560-2494

**FOR THE RESPONDENT:**

**CHR CORP. d/b/a Rutter's**

Date: 10/09/2023

By: \_\_\_\_\_


  
Scott Hartman  
President and CEO

2295 Susquehanna Trail Suite C,  
York, PA 17404

*Counsel to CHR CORP. d/b/a Rutter's*

Date: 10/11/2023

By: \_\_\_\_\_

  
Theodore J. Kobus III  
PA Attorney I.D. No. 73034

Craig A. Hoffmann  
Joseph L. Bruemmer  
Baker & Hostetler LLP  
312 Walnut Street  
Suite 3200  
Cincinnati, OH 45202



**IN THE COURT OF COMMON PLEAS OF  
YORK COUNTY, PENNSYLVANIA**

**COMMONWEALTH OF PENNSYLVANIA** :  
**By Attorney General Michelle A. Henry** :

**Petitioner** :

**v.** :


**CHR Corp. d/b/a Rutter's** :

**Respondent** :

**CERTIFICATE OF COMPLIANCE**

I, Timothy R. Murphy, certify that this filing complies with the provisions of the *Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts* that require filing confidential information and documents differently than non-confidential information and documents.

Date: October 10, 2023

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, 3<sup>rd</sup> Floor  
Philadelphia, PA 19103  
215-560-2414  
*Attorney for Petitioner*

**IN THE COURT OF COMMON PLEAS OF  
YORK COUNTY, PENNSYLVANIA**

**COMMONWEALTH OF PENNSYLVANIA** :  
**By Attorney General Michelle A. Henry** :

**Petitioner** :

**v.** :

**CHR Corp. d/b/a Rutter's** :

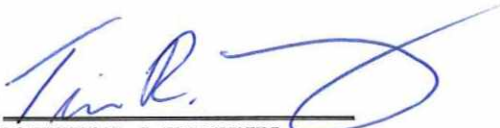
**Respondent** :

**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 CHR Corp. by serving Respondent's attorney, Theodore J. Kobus, III, Esquire at the following email address:

tkobus@bakerlaw.com

Date: October 10, 2023

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, 3<sup>rd</sup> Floor  
Philadelphia, PA 19103  
215-560-2414  
*Attorney for Petitioner*