1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

July 26, 2023

Via Email Only
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
Email: consumer@ag.iowa.gov

Re: HRM Enterprises, Inc. - Notice of Vendor Data Breach

Dear Sir or Madam:

We represent HRM Enterprises, Inc., a family of companies made up of the country's largest independent hardware store, and based in Hartville, Ohio. This submission is provided pursuant to the Iowa Personal Information Security Breach Protection statute, IOWA CODE ANN. §715C.1 *et seq*, which requires notice to your office in the event of a breach of the security of personal information affecting residents of the State of Iowa.

On June 8, 2023, HRM's e-commerce platform provider, Commerce V3, notified the company of a breach of Commerce V3's systems. The incident impacted the security of customers' payment card information used to make purchases from two HRM companies' e-commerce websites: Hartville Hardware and Lehman's. HRM took steps to confirm the risk to any data, including communicating with CommerceV3 for additional information about the incident. CommerceV3 advised it conducted a forensic investigation alongside third-party cybersecurity experts and discovered an unauthorized actor accessed its systems between November 24, 2021, and December 14, 2022. The unauthorized party potentially accessed or acquired payment card information entered within the platform during that timeline. CommerceV3 notes that it worked with the card companies to identify the payments entered during this window. HRM is notifying customers for whom CommerceV3's investigation determined made one or more payment card purchases via the platform during the period of unauthorized access. HRM concluded its investigation following notification from CommerceV3 on June 8, by July 10, 2023.

The potentially impacted information included customers' name and full payment card numbers, as well as email address, billing address, CVV code and expiration date for each purchase. Neither CommerceV3 nor HRM requires or stores Social Security number (SSN) for e-commerce transactions.

On July 26, 2023, HRM will begin providing, via U.S. regular mail and electronic mail, notice of this incident to potentially impacted individuals. A sample copy of the notice is attached as "Exhibit A" for your records. HRM will provide this notification to a total of 43,092 individuals, including 515 Iowa residents by email.

HRM is providing written notice of this event to the affected individuals that includes a brief description of the incident, encouragement to remain vigilant for incidents of payment card fraud or misuse, by reviewing and monitoring account statements and reporting any suspicious activity to the financial institution or issuing bank, and to file a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. HRM also enclosed documentation containing contact information for the major consumer reporting bureaus, state-specific regulators, a dedicated call center, and additional steps individuals may take to protect their information from misuse, should they find it appropriate to do so.

HRM moved quickly to investigate upon being notified by CommerceV3, including working with CommerceV3 to obtain additional information about the event so it could assess any risk to payment information. HRM continues to review its processes and policies and to make changes as necessary, including updating its vendor technical requirements and reassessing its vendor relationships. HRM is also notifying other regulators as required.

I believe this provides you with all information necessary for your purposes and to comply with Iowa law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

/s/ Nicholas Jajko

Nicholas Jajko

Exhibit A

[redacted]

From: IDX <reply@idxmail.us>
Sent: [redacted]M
To: [redacted]
Subject: Notice of Data Breach at Commerce V3

***Please do not reply back to this email with any personal information.**

July 26, 2023

Re: Notice of Data Breach at Commerce V3

Dear [redacted]:

HRM Enterprises, Inc. takes the privacy and security of your information seriously. In that regard, our e-commerce platform provider, CommerceV3, reported to us that certain card payment information you used to make purchases from <<Variable Data 1>> may be affected by a breach of their systems. Below is a summary of the event and steps you can take to protect your card information, should you feel it appropriate to do so. We partnered with IDX to provide you this notification, please read it carefully.

What Happened? On June 8, 2023, Commerce V3 notified our company of unauthorized activity CommerceV3 discovered on its systems, that impacted the security of our customers' payment information. We took steps to confirm the risk to any data related to purchases through <<Variable Data 1>> , including communicating with CommerceV3 for additional information about the incident. CommerceV3 advised it conducted a forensic investigation alongside third-party cybersecurity professionals and discovered an unauthorized actor accessed its systems between November 24, 2021, and December 14, 2022. The unauthorized party potentially accessed or acquired payment card information entered within the platform during that timeline. CommerceV3 notes that it worked with the card companies to identify the payments entered during this window. We are notifying you because CommerceV3's investigation determined you made one or more payment card purchases via the platform during the period of unauthorized access.

What Information Was Involved? The potentially impacted information included your name and <<Variable Data 2 ending in <<Variable Data 3>>, as well as email address, billing address, CVV code and expiration date for each purchase. Neither CommerceV3 nor HRM requires or stores Social Security number (SSN) for e-commerce transactions.

What We Are Doing. We moved quickly to investigate upon being notified by CommerceV3, including working with CommerceV3 to obtain additional information about the event so we could assess any risk to payment information. We continue to review our processes and policies and to make changes as necessary, including updating our vendor technical requirements and reassessing our relationships.

What You Can Do. We encourage you to remain vigilant against incidents of payment card theft and fraud by reviewing account statements and to alert your card company of suspicious activity and errors. We also encourage you to review the information contained in the below *Steps to You Can Take to Help Protect Information* section.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-888-220-6124, which is available from 9 am to 9 pm Eastern Time, Monday through Friday.

Sincerely,
HRM Enterprises, Inc.
1015 Edison St. NW
Hartville, OH 44362

STEPS YOU CAN TAKE TO HELP PROTECT INFORMATION

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report suspected fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Initial fraud alerts will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for up to seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online using the above contact information. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online using the above contact information. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- ***District of Columbia residents:*** District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; https://oag.dc.gov/; 202-727-3400.

- ***Maryland residents:*** Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; https://www.marylandattorneygeneral.gov/; or 1-410-528-8662 or 1-888-743-0023.
- ***New Mexico residents:*** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what information is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting bureaus may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to your employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have additional specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by contacting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580.
- ***New York residents:*** Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov; or 1-800-771-7755.
- ***North Carolina residents:*** North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; https://ncdoj.gov; and toll-free at (877) 566-7226 or (919) 716-6000.
- ***Rhode Island residents:*** Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; https://riag.ri.gov/; or 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in this matter. There are approximately 119 Rhode Island residents potentially impacted by this incident.
- ***All US Residents*:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261. This communication was not delayed by law enforcement.