



McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Eric R. Benson
Direct Dial: 248.593.2957
E-mail: ebenson@mcdonalddhopkins.com

January 10, 2025

VIA EMAIL (Idtheft@oag.state.md.us)

Anthony Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Scales Plus LLC – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Scales Plus LLC (“Scales Plus”). I am writing to provide notification of an incident potentially impacting Scales Plus that may affect the security of personal information for approximately as many as¹ nine (9) Maryland residents and/or corporations. By providing this notice, Scales Plus does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction

Scales Plus was recently informed by its e-commerce provider that, due to the compromise of a third-party application, payment card data entered onto the Scales Plus retail website (<https://www.scalesplus.com/>) between October 15, 2024, and November 7, 2024 may have been acquired by an unauthorized party.

Upon learning of this issue, Scales Plus commenced a prompt and thorough investigation. The investigation aimed to determine the Scales Plus customers whose payment card data may have been impacted in connection with an actual or potential purchase. Following an analysis of internal records, Scales Plus determined on December 11, 2024, that the personal information

¹ Note: an undetermined number of the potentially impacted payment cards may belong to businesses, not individuals

involved included a limited number of Maryland residents. The information included the impacted resident's full name and payment card information, including expiration dates and/or CVV codes.

To date, Scales Plus is not aware of any reports of identity fraud or improper use of information as a direct result of this incident. Nevertheless, Scales Plus wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Scales Plus is providing the potentially affected residents with written notification of this incident commencing on or about January 10, 2024 in substantially the same form as the letter attached hereto. Scales Plus is advising the potentially affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The potentially affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Scales Plus, protecting the privacy of personal information is a top priority. Scales Plus is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Scales Plus continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

If you have any additional questions, please contact me at (248) 593-2957 or ebenson@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink, consisting of a stylized 'EB' followed by a horizontal line.

Eric R. Benson

Encl.



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

Dear [Redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Scales Plus LLC (“Scales Plus”). We write to make you aware of a recent data security incident involving the potential unauthorized access to some of our customers’ payment card data used at our website <https://www.scalesplus.com/>.

What Happened?

We recently discovered that our online store was potentially modified with malicious code by a bad actor due to the compromise of a third-party application. The code may have captured certain payment card data as it was entered on our website by customers in connection with an actual or potential purchase.

What Information Was Involved?

Following an analysis of our internal records, we determined on December 11, 2024 that the personal information that may have been accessed and/or acquired as a result of this incident included your [Redacted]
[Redacted]
[Redacted]

What We Are Doing.

Because we value our relationship with you, we wanted to make you aware of the incident. Since learning of the incident, the impacted application has been remediated by the third-party application provider. Moreover, we are evaluating security measures taken by our third-party providers to enhance the security and privacy of your personal information.

What You Can Do

We have no evidence that your information has been used for identity fraud. Out of an abundance of caution, however, we wanted to make you aware of the incident. Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. As a best practice, you should also call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or card issuer whether a new card should be issued to you.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call Scales Plus at [REDACTED]

Sincerely,

Scales Plus

- OTHER IMPORTANT INFORMATION -

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 685-1111

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

*In Addition, New Mexico Consumers Have the Right to
Obtain a Security Freeze or Submit a Declaration of Removal*

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.