



2024 INDEPENDENCE COMMERCE AVENUE, SUITE E
MATTHEWS, NC 28105
704-628-7770

February 21, 2017

[Customer Name]
[Customer Address]
[Customer Address]

NOTICE OF DATA BREACH

Dear Customer:

We are writing to you because of an incident involving access to information associated with online purchases made on our website www.MovieMars.com. Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected customers about the incident, and about tools you can use to protect yourself against possible identity theft or fraud.

What Happened?

The MovieMars.com site is operated by a third-party company, Aptos, Inc. (our “platform provider”). We were informed on February 6, 2017 that the platform provider’s systems experienced an intrusion last year. The intruder or intruders placed malware on the platform provider’s services, and by doing so gained access to our customers’ payment card data. To date, the investigation indicates that the intrusion began in approximately February 2016 and ended in December 2016. The attackers gained access to customer information including payment card numbers as customers made transactions on the platform provider’s systems, and had access to historical payment card data. Because you have provided your payment card information to us in the past, we are notifying you about this data breach.

You may wonder why you are hearing about the breach now. The platform provider did not discover the breach until November 2016. In addition, law enforcement is investigating, and asked that notification to customers be delayed to allow the investigation to move forward.

What Information Was Involved?

The information that the attacker had access to includes your first and last name, address, phone number, and any debit or credit card numbers with expiration dates you may have used on our website.

What Are We Doing?

Our platform provider has worked with a leading cybersecurity firm to remove the malware from its systems and is actively monitoring the platform to safeguard personal information. Our platform provider has also contacted and offered its cooperation to federal law enforcement.

What You Can Do

Please be sure to review the enclosed “Additional Resources” section included with this letter. This section describes some additional steps you can take to help protect yourself (such as obtaining a copy of your credit report, or placing a security freeze on your credit report) and provides important contact information for the Federal Trade Commission, other law enforcement agencies, and credit reporting agencies.

In addition, we recommend you consider the following:

- **Contact Your Credit or Debit Card Issuer.** While we have taken steps to notify credit card processors, we recommend that you also immediately notify your credit card issuing bank and follow its advice with regard to your credit card.
- **Regularly Review Your Financial Statements.** We recommend you remain vigilant by regularly reviewing your credit card and bank account statements and monitoring free credit reports; and immediately alert your credit card issuing bank of any suspicious charges. This is one of the most important steps that you can take to detect and prevent any unauthorized use of your credit card number.
- **Be Aware of online “Phishing” Schemes.** You should also always be on the lookout for phishing schemes – emails where fraudsters pose as legitimate companies in order to trick people into disclosing personal information or clicking a link that causes the installation of malware. Any email correspondence we may send regarding this matter will not contain any clickable hyperlinks and will not ask you to reply with personal information. Never provide sensitive information to unsolicited requests claiming to come from us, your bank, or other organizations.

For More Information

We sincerely regret that this incident happened, and will continue to put the right measures in place to maintain the security of your information. For more information on preventing identity theft, please review the “Additional Resources” section.

ADDITIONAL RESOURCES

Obtain a Free Credit Report. We also recommend you remain vigilant by obtaining and reviewing your credit report. You may request a free copy of your U.S. credit report once every 12 months by visiting www.annualcreditreport.com or by calling 1-877-322-8228 toll free. You can print a copy of the request form at <https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>. You should review this for any information that is not accurate.

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Information on Credit Report Fraud Alerts. You also may place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

	Equifax	Experian	TransUnion
Phone	1-800-525-6285 or 1-888-766-0008	1-888-397-3742	1-800-680-7289
Address	Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp	https://www.experian.com/fraud/center.html	https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

Place a Security Freeze on Your Account. In addition to a fraud alert, you may also have a security freeze placed on your credit file. A security freeze will block a credit bureau from releasing information from your credit report without your prior written authorization. Please be aware that a security freeze may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. The fees for placing a security freeze vary by state, and a consumer reporting agency may charge a fee of up to \$10.00 to place a freeze or lift or remove a freeze. To place a security freeze on your credit report, you may send a written request to **each** of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting **each** consumer reporting agency online.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

	Equifax	Experian	TransUnion
Address	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp	https://www.experian.com/freeze/center.html	https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp

Contact Law Enforcement.

If you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission.

Federal Trade Commission. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. You can also call 1-877-ID-THEFT (877-438-4338) or write to Federal Trade Commission at 600 Pennsylvania Avenue, NW, Washington, DC 20580 for additional guidance. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcement for their investigations.

State-Specific Information.

For residents of Maryland, North Carolina, and Rhode Island: For information on how to avoid identity theft or to contact your state's attorney general, please use the below information.

For residents of Massachusetts and Rhode Island: Under Massachusetts and Rhode Island laws, you have the right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

	Maryland Attorney General	North Carolina Attorney General	Rhoda Island Attorney General	Massachusetts Attorney General
Phone	1-410-576-6491	1-877-566-7226 (within North Carolina)	1-401-274-4400	1-617-727-8400

		or 1-919-716-6000 (if outside North Carolina)		
Email	Idtheft@oag.state.md.us	consumer@ncdoj.gov	consumers@riag.ri.gov	AGO@state.ma.us
Address	Identity Theft Unit Attorney General of Maryland 200 St. Paul Place, 16th Floor Baltimore, MD 21202	Consumer Protection Division Attorney General's Office Mail Service Center 9001 Raleigh, NC 27699- 9001	Rhode Island Office of the Attorney General 150 South Main Street Providence, RI 02903	Massachusetts AGO One Ashburton Place Boston, MA 02108- 1518
Website	https://www.oag.state.md.us/	http://www.ncdoj.gov	http://www.riag.ri.gov	http://www.mass.gov/ago/