



Seth Berman

Direct Line: (617) 439-2338

Fax: (617) 310-9338

E-mail: sberman@nutter.com

March 2, 2021

108199-1

Via Breach Portal

Office of the Maine Attorney General
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Sir or Madam:

My firm represents Strat-O-Matic Media, LLC (“Strat-O-Matic”), a producer of sports-simulation games, of 42 Railroad Plaza Glen Head, NY 11545. Pursuant to 10 M.R.S.A. §§1346-1350-B, I am writing to notify you of a data breach involving the personal information of thirty-two Maine residents.

On Monday, February 8, 2021, Strat-O-Matic discovered that an unauthorized third-party intercepted credit or debit card information of customers who made purchases at Strat-O-Matic. An investigation by third-party experts determined that this started on January 5, 2021 and ended when Strat-O-Matic learned of and took steps to correct the problem on February 8, 2021. As a result of this attack, hackers had access to customers’ first and last name, address, and any debit or credit card numbers with expiration dates and security codes used to make purchases at Strat-O-Matic from January 5, 2021 to February 8, 2021.

As noted above, Strat-O-Matic learned about the incident on February 8, 2021. Once it did, it moved as rapidly as possible to notify the affected population, initially in a series of emails to affected individuals, the first of which was sent that same day, and then subsequently by posting publicly about it on its website. Strat-O-Matic has been informed by several customers that credit or debit card information implicated in this incident was used in attempted fraudulent transactions. Strat-O-Matic further notified affected individuals by written notice on March 2, 2021. A copy of that notice is attached to this letter. Finally, on February 24, 2021, Strat-O-Matic filed a report with the Federal Bureau of Investigations through the Bureau’s Internet Crime Complaint Center.

As part of Strat-O-Matic’s ongoing efforts to help prevent something like this from happening in the future, the company has stopped accepting credit and debit cards directly. Going forward at Strat-O-Matic, either on its website or via phone order, customers will be able to use either debit or credit cards through PayPal or Amazon Pay, where their payment card information is protected by PayPal or Amazon’s security. Strat-O-Matic has also engaged a



March 2, 2021

Page 2

third-party security organization which has determined what happened and has taken steps to prevent similar events in the future.

As noted above, the only information involved in this incident was residents' first and last name, address, and debit or credit card information. Strat-O-Matic does not collect customer social security numbers or birthdates, and this data was not and could not have been involved in this incident. Nevertheless, Strat-O-Matic will be offering all Maine residents whose credit or debit card information was potentially affected identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services to help alleviate any concerns they may have resulting from this incident and to help prevent misuse of any information.

Please do not hesitate to contact me if you have any questions.

Very truly yours,

A handwritten signature in blue ink, appearing to read "S. Berman", with a long horizontal flourish extending to the right.

Seth Berman

SPB2:jwg2

Enclosure

5081312.3



C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-933-1097
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

<<First>> <<Last>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Breach

Dear <<First>> <<Last>>,

At Strat-O-Matic Media, LLC, we take the security of our community members' information very seriously. This letter is a follow up to the emails and public announcements we have made regarding an incident that impacted the credit or debit card information you used for purchases between January 5, 2021 and February 8, 2021. We sincerely apologize for any inconvenience this incident may cause and are writing this letter to inform you about steps you can take to protect your information and resources we are making available to you.

What Happened

On Monday, February 8, 2021, Strat-O-Matic discovered that an unauthorized third-party intercepted credit or debit card information of customers who made purchases at Strat-O-Matic. An investigation by third-party experts determined that this started on January 5, 2021 and ended when Strat-O-Matic learned of and took steps to correct it on February 8, 2021. As a result of this attack, hackers obtained credit or debit card information from transactions occurring during the relevant time period. Sadly, we join a long list of companies (large and small) who have had customer information stolen.

This attack only impacted individuals who made purchases during that period, and only if they used our payment system (this is for both orders made on our website AND phone orders as our operators use our website to place those orders that are called in). Customers who purchased using PayPal – even if they used a credit card with PayPal to complete the transaction – were not impacted by this incident. Similarly, customers who completed their payments prior to January 5, 2021 or after February 8, 2021 were not impacted.

What Information Was Involved

The information that the attacker had access to includes your first and last name, your address, and any debit or credit card numbers with expiration dates and security codes you may have used to make purchases at Strat-O-Matic from January 5, 2021 to February 8, 2021.

According to our records, you made a payment card purchase during that timeframe, and we therefore believe that your information is at risk.

What We Are Doing

Through this letter, our prior emails, and public notices, we are letting you know about the incident so that you can take immediate action to protect yourself, as detailed below.

As part of our ongoing efforts to help prevent something like this from happening in the future, we have stopped accepting credit and debit cards directly. Going forward at Strat-O-Matic, either on our website or via phone order, customers will

be able to use either debit or credit cards through PayPal or Amazon Pay, where their payment card information is protected by PayPal or Amazon's security. You do not need to have an account with either PayPal or Amazon to complete your purchase. We have also engaged a third-party security organization which has determined what happened and has taken steps to prevent similar events in the future.

What You Can Do

Because this incident may have impacted the credit or debit card you used, we recommend that you contact your credit or debit card company and inform them of this incident so that they can take steps to prevent your card number from being misused. We strongly recommend canceling the card that you used at Strat-O-Matic. We also recommend that you remain vigilant and promptly report any suspicious activity or suspected fraud or theft to the proper law enforcement authorities.

To further assist you in this process we have attached a sheet of **Recommended Steps** that we suggest you consult.

As noted above, the only information involved in this incident was your first and last name, your address, and your debit or credit card information as detailed above. Strat-O-Matic does not collect customer social security numbers or birthdates, and this data was not and could not have been involved in this incident. However, in order to ensure that you feel further protected from any potential impact, Strat-O-Matic is offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To receive credit monitoring you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-933-1097 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 2, 2021.

For More Information

You will find detailed instructions for enrollment on the enclosed **Recommended Steps** document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-933-1097 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Thanks for your understanding and continued patronage.

Sincerely,



Harold Richman
Chief Executive Officer

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-933-1097 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. 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 1-877-322-8228. 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 and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file and obtain a copy of 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General. You have the right to obtain any police report filed in regard to this incident.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you may also send a written request by regular, certified or overnight mail to the addresses above.

The credit reporting agencies will provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or go online to each of the credit reporting agencies and provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the specific period of time you want the credit report available. The credit reporting agencies will lift the security freeze for the specified period of time.

To remove the security freeze, you must call or go online to each of the three credit bureaus and provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus will remove the security freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia Residents: Office of the Attorney General of the District of Columbia, 400 6th Street, NW, Washington, DC 20001; Phone: (202) 727-3400; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: oag@dc.gov

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: You may place a security freeze on your credit reports, free of charge. In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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 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 agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to 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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400. Residents may contact the FTC or the North Carolina Attorney General's Office for further information about preventing identity theft

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. This incident involved nineteen Rhode Island residents.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261. You can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

