

Kennedys

Our ref: USY104.1078909

Via Certified Mail/Return Receipt Requested

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

570 Lexington Avenue
8th Floor
New York, NY 10022
USA

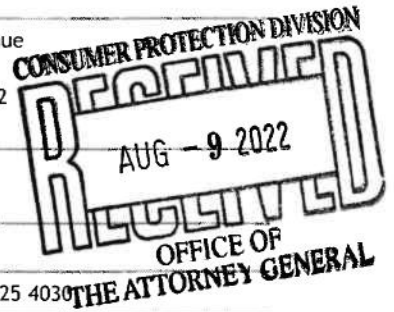
t +1 212.252.0004
f +1 212.832.4920

kennedyslaw.com

Direct Dial +1 646 625 4030

Daniel.Marvin@kennedyslaw.com

August 1, 2022



Re: Notice of Breach of a Security System

Dear Sir/Madam:

We write on behalf of Yellow Social Interactive Limited (YSI), a Gibraltar company having its registered office at 2 Irish Town, Gibraltar, GX11 1AA, to provide notice of a Breach of a Security System, as that term is defined by Md. Code Ann. Comm. Law 14-3504.

Number of Affected Individuals in Maryland

The incident involved the information of 240 Maryland residents.

Description of Breach of Security of System

On or about April 27, 2022, YSI received a communication from an unknown party identifying himself as a bug bounty detectorist. The individual told YSI that he had found an application programmable interface (API) vulnerability and that he had accessed data from a supporting database. To prove his access, the individual provided screen shots of data with names and states. YSI immediately investigated the vulnerability and fixed it. YSI also retained counsel, and through counsel, engaged a third-party forensic firm to investigate the incident and confirm the security of its systems.

Further investigation confirmed that the driver license numbers, or in some limited instances, passport numbers instead, for some customers also was impacted, and that the individual had copied some data to prove the existence of the "bug." No other Personally Identifiable Information (PII) was accessed in connection with the incident. The individual destroyed any data he possessed to prove existence of the "bug." There is no ongoing threat. We have found no other instances of malicious activity in our systems in connection with the incident, and YSI has no evidence that the impacted data has been used for fraudulent purposes.

Steps Taken Relating to Breach of Security of System

YSI immediately investigated the vulnerability and fixed it. YSI also retained counsel, and through counsel, engaged a third-party forensic firm to investigate the incident and confirm the security of its systems. YSI also is provide notice to Maryland consumers whose PI was impacted. A template of the notice being sent is enclosed.

Additional questions may be directed to my attention. Thank you.

Very truly yours,

Daniel S. Marvin

Daniel S. Marvin
Partner
For Kennedys

Enclosure

Notice of A Data Breach

Dear Pulsz Customer

Yellow Social Interactive writes to inform you of an IT security incident from a bug bounty detectorist that may have impacted some personal information that you provided to us. This correspondence provides you with information about the incident, our response, and additional steps you may take should you determine it appropriate.

What Happened?

On or about April 27, 2022, YSI received a communication from an individual identifying himself as a bug bounty detectorist. Such individuals look for IT vulnerabilities or “bugs,” and inform companies of them in the hope for an award or “bounty.” Here, the individual told YSI that he found an application programmable interface (API) vulnerability that allowed him to access data from a supporting YSI database. The individual initially provided YSI with screenshots of the allegedly accessed data, and even copied some data, to prove existence of the bug. YSI immediately investigated the vulnerability and fixed it, and the individual destroyed any data he possessed. There is no ongoing threat, and we have no evidence that any data has been misused for fraudulent purposes. Law enforcement was not notified. Nevertheless, YSI is informing players whose personal information may have been involved.

What Type of Information Was Involved

The personal information potentially involved were names, driver’s license number and state or in some limited instances passport number.

What We Are Doing

We are reaching out to notify you about the event. We have fixed the bug.

What You Can Do

Please see Appendix A below.

Further Information

We collected further information at the end of this email if you want to remain vigilant and protect yourself. Your account security is important to us and if you have any questions about this, you may contact us on notifications@ysi-group.com or by phone at [+1 \(424\) 371-7304](tel:+14243717304).

Sincerely,
Your YSI team

Appendix A

Placing a Fraud Alert on Your Credit File

You may take some of these steps to remain vigilant should you think it. You may, free of charge, place an initial 1-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 www.equifax.com 1-800-525-6285	Experian P.O. Box 2002 Allen, TX 75013 www.experian.com 1-888-397-3742	TransUnion LLC P.O. Box 2000 Chester, PA 19016 www.transunion.com 1-800-680-7289
--	---	---

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 sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.freeze.equifax.com 1-800-685-1111	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742	TransUnion Security Freeze P.O. Box 2000 Chester, PA 19016 http://www.transunion.com/securityfreeze 1-888-909-8872
---	--	--

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 monitoring 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. If you do

place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

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.

Additional 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.