Attorney General Bob Ferguson
SecurityBreach@atg.wa.gov

April 1, 2021

Dear Attorney General Ferguson,

I write on behalf of my client, MHNext, LLC (d/b/a Manhunt) ("Manhunt") to inform you of an incident affecting the personal information of approximately 7714 Washington residents. On March 2, 2021, Manhunt discovered that an attacker had gained access to a database that stored account credentials for Manhunt users. The attacker downloaded the usernames, email addresses and passwords for a subset of our users in early February 2021.

Manhunt immediately took steps to remediate the threat and secure its systems. Passwords were forced-reset for affected user accounts, and we retained a third-party forensics consultant on behalf of Manhunt to assist us in investigating what happened and confirm that there is no ongoing unauthorized access to Manhunt systems.

Manhunt takes the security of its users' information very seriously. In accordance with state law, we are notifying affected residents regarding this incident via email and a message in our users' inboxes on our platform. Manhunt began to send notices on March 16, 2021, and will continue to send them through this week on a rolling basis as it works with a third-party service to refresh its email list. A sample notice is attached. Should you have further questions about this matter, please contact me at stacey@zwillgen.com.

Sincerely,

Stacey Brandenburg

NOTICE OF DATA BREACH

March 17, 2021

We are writing to notify you of a security incident affecting the security of your Manhunt account credentials.

What Happened?

On March 2, 2021, Manhunt discovered that an attacker gained access to a database that stored account credentials for Manhunt users. The attacker downloaded the usernames, email addresses and passwords for a subset of our users. We immediately took steps to remediate the threat and reset the passwords of affected users.

What Information Was Involved?

The data elements accessed by the unauthorized attacker included your Manhunt username, password, and email address used to register your account. We have no evidence that users' pictures, messages, or other profile information were acquired by the attacker. As we do not transmit or store any payment card information, **no payment card information was exposed as a result of this incident**.

What We Are Doing

Manhunt takes your privacy and security seriously. When we discovered this incident, we immediately took steps to contain the intrusion and remediate the threat that led to the unauthorized access. We also reset the passwords for affected user accounts and retained a third-party forensics consultant to assist us in investigating what happened and confirm that there is no ongoing unauthorized access to our systems.

What You Can Do

We have reset your account password. So, if you haven't done so already, you will be prompted to create a new password the next time you log in. We strongly encourage you to select a unique password that you have not used for another website or account. If you used your previous Manhunt account password on other sites, we urge you to change those passwords as well.

Additionally, be vigilant for "phishing" messages purporting to be from Manhunt or claiming to have information about your Manhunt account. Manhunt will never ask you for your password or other sensitive information via email. You should also never click on links in emails from senders you do not know. If you notice any unusual activity on your Manhunt account or if you receive any unusual communication purporting to be from Manhunt, please contact us using the contact information below.

For More Information

We sincerely regret any inconvenience this incident may have caused. If you have any questions regarding this incident, please contact Manhunt at support@manhunt.net. While we have no reason to think that this incident exposed any information that could be used to commit identity theft, certain state laws require us to provide you with information about preventing and reporting identity theft. You can find that information below.

****

SUPPLEMENTAL INFORMATION

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-685-1111	1-888-397-3742	1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

State Attorneys General
Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.

If you are a resident of California, Connecticut, Iowa, Maryland, Massachusetts, North Carolina, Oregon, or Rhode Island, you may contact and obtain information from and/or report identity theft to your state attorney general at:

California Attorney General's Office, California Department of Justice, Attn: Office of Privacy Protection, P.O. Box 944255, Sacramento, CA 94244-2550, (800) 952-5225

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-576-6300

Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or 1-877-566-7226

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (503) 378-4400, http://www.doj.state.or.us/

Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If you are a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze	**TransUnion Security Freeze**	**Equifax Security Freeze**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
www.experian.com	www.transunion.com	www.equifax.com

To request a security freeze, you will need to provide the following information:

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 years, provide the addresses where you have lived over the prior five years

5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and 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, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include 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 have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.