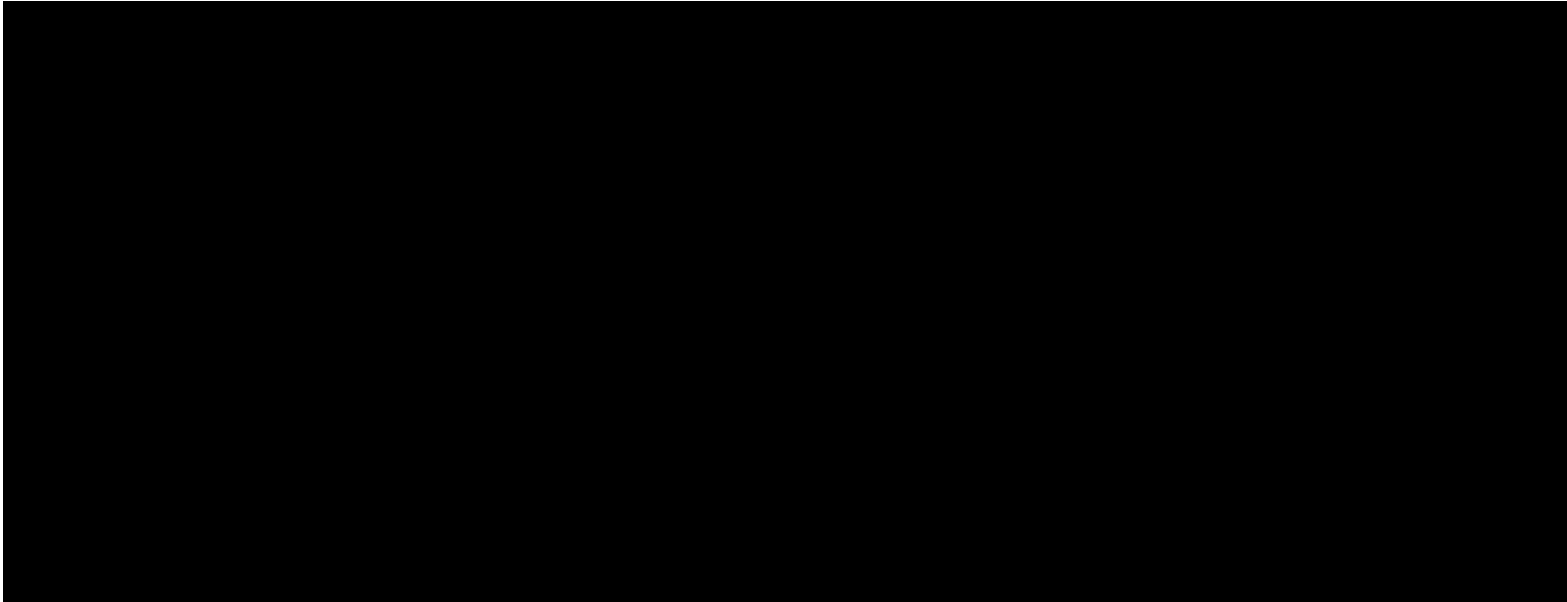




Dear Office of the Attorney General,

We are reporting a data breach of Mansueto Ventures impacting two Maryland residents.

A brief description of the breach:

From September 25 to September 27, 2022, Fast Company's content management system (CMS) experienced a cyberattack. An unauthorized individual gained access to CMS during that time, which resulted in certain data being extracted from the CMS. On September 28, 2022 Mansueto Ventures, the parent company of Fast Company, engaged a cybersecurity firm to investigate the incident. The cybersecurity firm discovered a copy of the Fast Company CMS user database that was posted publicly for sale on the Breach Forums website (<https://breached.to>). The cybersecurity firm has determined that some personal information was included in the CMS database made available for sale on Breach Forums, specifically user names and display names, email addresses, hashed passwords, and login IP addresses.

A copy of our consumer notice is attached. It will be issued October 13, 2022.

Please contact me with any questions or concerns.

Thank you,

Mark Rosenberg
CFO
Mansueto Ventures
(212) 389 3223

October 13, 2022

NOTICE OF DATA BREACH

Dear [[insert name]],

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

What Happened?

From September 25 to September 27, 2022, *Fast Company's* content management system (CMS) experienced a cyberattack. An unauthorized individual gained access to CMS during that time, which resulted in certain data being extracted from the CMS. On September 28, 2022 Mansueto Ventures, the parent company of *Fast Company*, engaged a cybersecurity firm to investigate the incident. The cybersecurity firm discovered a copy of the *Fast Company* CMS user database that was posted publicly for sale on the Breach Forums website (<https://breached.to>). The cybersecurity firm has determined that some of your personal information was included in the CMS database made available for sale on Breach Forums

What Information Was Involved?

The personal information included in database made available for sale included the following:

- Your *Fast Company* WordPress user name and display name;
- Your *Fast Company* WordPress email address;
- Your hashed *Fast Company* WordPress password;
- The IP address of your last log-in to the *Fast Company* WordPress database made prior to September 25, 2022.

What We Are Doing

We take the privacy and security of data seriously. Mansueto Ventures has reported the incident to the US Federal Bureau of Investigation and is cooperating with their investigation into the incident. There has been no delay in this Notice due to the ensuing investigation.

The cybersecurity firm engaged by Mansueto Ventures is monitoring all Mansueto Ventures' websites.

Although there is no evidence that your personal information has been fraudulently used, Mansueto Ventures is offering enrollment in one year (12 months) of complimentary LifeLock Standard Identity Theft Protection services.

What You Can Do

While the passwords made available for sale in this incident were hashed, we are encouraging you to change your passwords to any web sites, accounts, programs or applications, especially those with similar or the same user name, display name, or password to your Fast Company WordPress account.

You can also enroll in one year (12 months) of complimentary LifeLock Standard Identity Theft Protection, upon request. In order to request this service, please contact me at:

Mark Rosenberg
Mansueto Ventures
7 World Trade Center 29th Floor
New York, NY 10007

or call me at (212) 389-5223 from 9:00am to 5:00pm EST.

You can also follow the recommendations included in this letter, including those in the “Steps You Can Take to Further Protect Your Information” section below, which includes resources and information about how to protect your personal information.

For More Information.

If you have any questions about this letter, please contact me at:

Mark Rosenberg
Mansueto Ventures
7 World Trade Center 29th Floor
New York, NY 10007

or call me at (212) 389-5223 from 9:00am to 5:00pm EST.

We appreciate your patience and understanding on this matter.

Very Truly Yours,

Mark Rosenberg
CFO
Mansueto Ventures

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Credit Reports: Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. You are also entitled to a free credit report once every 12 months from each of these agencies at www.annualcreditreport.com, call toll-free 877-322-8228 or by completing an Annual Credit Request Form at www.ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing to:

Annual Credit Report Request Service,
P.O. Box 1025281
Atlanta, GA 30348-5283.

You can also obtain a credit report by contacting one of the following three national credit reporting agencies by phone and online:

Equifax: equifax.com/personal/credit-report-services or 1-800-685-111	Experian: experian.com/help or 1-888-397-3742	TransUnion: transunion.com/credit-help or 1-888-909-8872
--	---	--

When you receive your credit reports, review your credit reports for accounts and inquiries you don't recognize, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. These can be signs of identity theft. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report.

You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC) at the FTC address, phone number or website listed for the FTC above in the **"Review Your Account Statements and Notify Law Enforcement of Suspicious Activity"** section.

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

Fraud Alerts: The Federal Trade Commission (FTC) recommends that you place a free 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. Contact any one of the three major credit bureaus using the contact information below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert is free and stays on your credit report for one year. You can renew it after one year. Additional information is available at <http://www.annualcreditreport.com>.

Equifax https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf	Experian https://www.experian.com/fraud/center.html	TransUnion https://www.transunion.com/fraud-alerts
---	--	--

Credit Freeze: You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a freeze, contact each of the major credit bureaus using the information below. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 https://www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 https://www.transunion.com/credit-freeze
---	--	---

In order 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 (5) years, provide the addresses where you have lived over the prior five (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) business day after receiving a telephone or secure electronic request, or three (3) business days after receiving your written request, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including 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 identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must 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 have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

For Maryland residents: You may obtain additional information about how to avoid identity theft by contacting the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov/>, 1-888-743-0023.

For Massachusetts residents: Under Massachusetts law, you have the right to obtain any 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.

For New York residents: You may also obtain information about preventing and avoiding identity theft from by visiting the following websites:

New York State Department of State Division of Consumer Protection:
<https://dos.nysits.acsitefactory.com/consumer-protection>

New York State Attorney General at: <http://www.ag.ny.gov/home.html>

For more information on placing a security freeze on your credit reports, please go to the New York Department of State Division of Consumer Protection website at

<https://dos.nysits.acsitefactory.com/consumer-protection>.

For North Carolina residents: You may obtain additional information by contacting the North Carolina Office of the Attorney General, Mail Service Center 9001, Raleigh, NC 27699-9001, <http://www.ncdoj.gov/>, 1-877-566-7226. You can obtain further information on preventing identity theft and next steps for any suspected incidence of identity theft or fraud by visiting the Consumer Protection Division of the North Carolina Office of the Attorney General's "Security Breach Advice" at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id-theft/security-breach-information/security-breach-advice/>.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and:

Oregon Division of Consumer Protection of the Department of Justice:

<https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/>.

Oregon Division of Financial Regulation: <https://dfr.oregon.gov/Pages/index.aspx>.

For Virginia residents: You may obtain additional information by contacting the following websites:

Attorney General of Virginia: <https://www.oag.state.va.us/>.

Virginia Consumer Protection Agencies:

<https://www.oag.state.va.us/CCSWeb2/index.php/identity-theft/consumer-protection-agencies>.

For Washington D.C. residents: You may obtain additional information by contacting the: District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 2000 Phone: (202) 727-3400; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: oag@dc.gov or contact OAG's Office of Consumer Protection at 202-442-9828.