



Liberty Building, 420 Main Street, Suite 1110, Buffalo, New York 14202
3 Columbus Circle, #1500, New York, New York 10019
600 Broadway, Suite 700, San Diego, California 92101
2 Bala Plaza, Suite 300 #704, Bala Cynwyd, Pennsylvania 19004
75 S. Clinton Ave, 510 Clinton Square, Suite 555, Rochester, New York 14604

May 27, 2021

VIA EMAIL

Office of the Idaho Attorney General
Consumer Protection Division
700 W. Jefferson Street
Boise, ID 83720-0010
agwasden@ag.idaho.gov

Dear Sir or Madam:

On behalf of our client Accucom Corporation (“Accucom”) we provide this letter to your office as notice of a recent data security incident.

On December 16, 2020, Accucom became aware of the existence of unauthorized code running on its websites’ databases. Accucom immediately removed the code, notified the FBI, reconfigured access controls, changed passwords, and retained national data security experts. Accucom confirmed that from May 25, 2020 through December 16, 2020, the unauthorized code may have copied Accucom customers’ names and credit card details. No social security numbers or other financial account information were at risk. After conducting its investigation, Accucom was able to determine the extent of the data security incident, the number of affected individuals, as well as identity of individuals on May 14, 2021.

A total of 301,065 individuals, including 1,685 Idaho residents, may have been affected by this data security incident. Accucom does not collect its customers’ addresses but did not want to rely entirely on substitute notice so it engaged in lengthy requests for assistance from all the credit card issuers involved. All but one credit card brand refused assist in mailing notices to potentially affected individuals, resulting in notice being mailed to 45 Idaho residents. Individual notice to these 45 Idaho residents was provided on May 27, 2021. With regard to the remaining affected individuals who Accucom was unable to identify mailing addresses for, Accucom provided these individuals notice via email, mass media notice, and a posting on the Accucom website. A copy of the mailed letter and emails provided to potentially affected Idaho residents is attached hereto.

Please feel free to contact me with any questions at 716-898-2102 or dgreene@beckage.com.

Sincerely,

Daniel P. Greene, Esq.
Certified Information Privacy Professional, United States (CIPP/US)
Certified Information Privacy Professional, Europe (CIPP/E)

Encls.

May 27, 2021



Dear [REDACTED],

We write to advise you that we were recently the victim of a data security incident (the “Incident”). We are writing to let you know how this Incident may have affected your personal information (“Information”) and, as a precaution, to provide steps you can take to help protect your Information. We are contacting you to share what we know about the Incident.

What Happened?

On December 16, 2020, we learned that unauthorized code was deployed in our system in an attempt to capture our customers’ information, including names and credit card details. Some customers who used Infotracer.com, RecordsFinder.com, or StateRecords.org were affected. Upon learning of this, we immediately removed the unauthorized code, changed passwords, alerted law enforcement, and retained national data security experts. Our investigation revealed that the Incident may have involved your Information.

What Information Was Involved?

It is important to note that only limited information about you may have been involved: your name, email address, and credit card details. No other information about you was at risk.

What We Are Doing.

We immediately investigated the matter and continue to implement appropriate measures to further improve the security of our systems and practices. We are working with a leading data security firm to aid in our investigation and response and will report this Incident to relevant state authorities, as required. We also implemented additional security protocols designed to protect our systems and personal information.

What You Can Do.

It is always recommended that you regularly review account statements and report any suspicious activity to financial institutions. Please also review the enclosed “Additional Resources” section included with this letter, which describes additional steps you can take to help protect your Information.

As an added precaution to help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by August 31, 2021** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/credit>
- For a full year of service free for you, provide this **activation code**: [REDACTED]

If you have questions or need assistance enrolling, please call (855) 896-4452 by **August 31, 2021**. Be prepared to provide **engagement number** [REDACTED] as proof of eligibility for the identity restoration services by Experian.

For More Information.

If you have any questions please call (855) 896-4452 Monday through Friday, from 9:00 a.m. to 11:00 p.m. Eastern Standard Time. Saturday and Sunday 11:00 am to 8:00 pm Eastern Standard Time (excluding some U.S. national holidays).

Sincerely,



Levon Gasparian

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

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

May 27, 2021

Dear [REDACTED],

We write to advise you that we were recently the victim of a data security incident (the “Incident”). We are writing to let you know how this Incident may have affected your personal information (“Information”) and, as a precaution, to provide steps you can take to help protect your Information. We are contacting you to share what we know about the Incident.

What Happened?

On December 16, 2020, we learned that unauthorized code was deployed in our system in an attempt to capture our customers’ information, including names and credit card details. Some customers who used Infotracer.com, RecordsFinder.com, or StateRecords.org were affected. Upon learning of this, we immediately removed the unauthorized code, changed passwords, alerted law enforcement, and retained national data security experts. Our investigation revealed that the Incident may have involved your Information.

What Information Was Involved?

It is important to note that only limited information about you may have been involved: your name, email address, and credit card details. No other information about you was at risk.

What We Are Doing.

We immediately investigated the matter and continue to implement appropriate measures to further improve the security of our systems and practices. We are working with a leading data security firm to aid in our investigation and response and will report this Incident to relevant state authorities, as required. We also implemented additional security protocols designed to protect our systems and personal information.

What You Can Do.

It is always recommended that you regularly review account statements and report any suspicious activity to financial institutions. Please also review the enclosed “Additional Resources” section included with this letter, which describes additional steps you can take to help protect your Information.

As an added precaution to help protect your identity, we are offering **a complimentary one-year membership to IDStrong**, an identity restoration and credit-monitoring service.

[CLICK HERE TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION!](https://www.idstrong.com/monitor)

<https://www.idstrong.com/monitor>

Your individual activation code is:

- [REDACTED]
- Ensure that you enroll by **August 31, 2021** (Your code will not work after this date.)

For More Information.

If you have any questions, our care team is available 24/7 and eager to help. Please call (855) 941-4736 to reach an expert.

Sincerely,



Levon Gasparian

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

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