

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

July 30, 2024

Dear Mr. Attorney General:

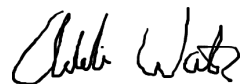
Etison LLC dba ClickFunnels (“Etison”, “we”, and “our”) recently detected a data security incident impacting certain checkout pages present on our platform. We are contacting you directly because **six (6) Maryland residents** input their personal information into a potentially compromised checkout step on our website between July 21, 2024 and July 24, 2024. Some personal information may have been impacted in this incident. We do not have evidence of any misuse of such personal information at this time.

On July 24, 2024, we became aware of a malfunctioning checkout page on our platform. Within minutes, we activated our Incident Response Plan to initiate an investigation of the incident. The investigation indicated that an unauthorized individual was able to inject custom code into the footer script of an Etison webpage by gaining access to one of our third-party contractor’s platform login credentials. After auditing internal records and logs for the affected webpage, we were able to determine that the unauthorized access occurred on July 21, 2024, at 4:36 a.m. Mountain Time. The custom code remained active on our webpage until July 24, 2024, at 3:58 p.m. Mountain Time, at which time we removed the custom script.

Upon discovery of the incident, we audited and remediated our environment, disabled the compromised contractor’s account, and implemented additional security measures for our authorized individuals.

Attached is a copy of the sample notice that we will be sending to the affected Maryland residents on August 1, 2024. If you have any questions or concerns, please do not hesitate to contact me at legal@clickfunnels.com or (208) 391-3460.

Sincerely,



Addison Watson
General Counsel, ClickFunnels

[<<NOTICE DATE>>]

Notice of Data Breach

Dear Consumer,

Etison LLC dba ClickFunnels (“Etison”, “we”, and “our”) recently detected a data security incident impacting certain checkout pages present on our platform. We are contacting you directly because you input your personal information into a potentially compromised checkout step on our website between July 21, 2024 and July 24, 2024. Some of your personal information may have been impacted in this incident. Please read this notice carefully, as it contains important information for consumers regarding the security incident including, what happened, what remedial actions we have taken, and ways that you can protect your personal information.

What Happened?

On July 24, 2024, we became aware of a malfunctioning checkout page on our platform. Within minutes, we activated our Incident Response Plan to initiate an investigation of the incident. The investigation indicated that an unauthorized individual was able to inject custom code into the footer script of an Etison webpage by gaining access to one of our third-party contractor’s platform login credentials. After auditing internal records and logs for the affected webpage, we were able to determine that the unauthorized access occurred on July 21, 2024, at 4:36 a.m. Mountain Time. The custom code remained active on our webpage until July 24, 2024, at 3:58 p.m. Mountain Time, at which time we removed the custom script.

What Information Was Involved?

The information involved may include your name, email address, phone number, physical address, and credit card information.

What Are We Doing?

Upon discovery of the incident, we audited and remediated our environment, disabled the compromised contractor’s account, and implemented additional security measures for our authorized individuals. We are also notifying you so that you may take further steps to protect your information, should you feel it appropriate to do so.

What You Can Do

We regret any inconvenience this may cause and are informing you about this issue promptly so you can take steps to help protect your information. Steps you can take include:

- **Order a Credit Report.** You are entitled under United States law to one free credit report annually from each of the three nationwide credit reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at (877) 322-8228.
- **Remain Vigilant.** We encourage you to review your account statements for suspicious activity and monitor your free credit reports.
- **Review the Following Reference Guide.** The attached Reference Guide provides information and recommendations on the protection of personal information.

More Information

If you have any questions regarding this incident or would like to understand what personal information of yours is maintained by us, please email incidentresponse@clickfunnels.com or call +1(208)-391-6395 Monday through Friday from 10:00 a.m. to 4:00 p.m. Mountain Time, excluding federal holidays. We take this matter very seriously. Please refer to the attached Reference Guide for additional information and resources. Please accept our sincere apologies for any inconvenience that this may cause you.

Sincerely,

Addison K. Watson
General Counsel, ClickFunnels
3443 West Bavaria Street
Eagle, Idaho 83616

Reference Guide

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your relevant financial institution or payment card company. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

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

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that

allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	(800) 525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	(888) 397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	(800) 680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Connecticut Residents. You may contact and obtain information from your state attorney general at:

Connecticut Attorney General’s Office
165 Capitol Avenue
Hartford, CT 06106
1-866-808-5318
www.ct.gov/ag

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity theft. This office can be reached at:

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

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act (“FCRA”). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
(800) 771-7755
(800) 788-9898
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology>

For North Carolina Residents. You can obtain information from the North Carolina Attorney General’s Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General’s Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
(919) 716-6400

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392
(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)727-3400
www.oag.dc.gov