

Clayton Northouse
Direct Dial: 202-637-3371
clayton.northouse@lw.com

555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Tel: +1.202.637.2200 Fax: +1.202.637.2201
www.lw.com

LATHAM & WATKINS LLP

FIRM / AFFILIATE OFFICES

Austin	Milan
Beijing	Munich
Boston	New York
Brussels	Orange County
Century City	Paris
Chicago	Riyadh
Dubai	San Diego
Düsseldorf	San Francisco
Frankfurt	Seoul
Hamburg	Shanghai
Hong Kong	Silicon Valley
Houston	Singapore
London	Tel Aviv
Los Angeles	Tokyo
Madrid	Washington, D.C.

May 15, 2024

VIA EMAIL

Office of the Attorney General
State of Maryland
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Security Breach Notification

Dear Mr. Brown,

I am writing on behalf of Interactive Brokers LLC (the “Company”) to provide you with information about a business email compromise impacting a small number of residents of Maryland.

On or around January 11, 2024, the Company identified a business email compromise that resulted in the unauthorized access to a limited amount of consumer personal information. Based on the Company’s subsequent investigation and forensic review, the Company determined the first activity relating to the business email compromise occurred on or around October 30, 2023, although the Company did not identify suspicious activity until January 11, 2024. As soon as the Company became aware of the unauthorized access, it activated its incident response protocols and implemented containment and remediation measures to ensure the security of the Company’s email environment, including the revocation of session tokens and resetting employee account credentials on all impacted accounts.

Based on the forensic review, the Company determined that the incident was contained to four email accounts, a very small portion of the Company’s overall email environment. With the assistance of its outside law firm and a data analytics firm, the Company conducted an analysis of the impacted data, which consisted of an extensive manual review of impacted files and information.

The data analytics firm provided its findings on April 30, 2024, and, on May 2, 2024, the Company was able to determine the specific individuals and data elements impacted by the incident and the Company’s notification obligations.

Based on the forensic review, the Company identified that four (4) Maryland residents were impacted. The Company will start notifying individuals affected by this incident by direct mail. The Company is offering two-year credit monitoring and identity protection services through Experian for all impacted individuals. A copy of the notification to customers is attached to this letter.

The Company notified federal law enforcements of the incident on April 18, 2024. Data

LATHAM & WATKINS LLP

privacy and security are among the Company's highest priority, and the Company has extensive measures in place to help protect information in the Company's care. The Company trains its employees on an ongoing basis regarding cybersecurity best practices and the risk of phishing, and is committed to continuously reviewing and enhancing its security environment.

If your office requires any further information regarding this matter, please contact me at (202) 637- 3371 or clayton.northouse@lw.com.

Respectfully submitted,

A handwritten signature in blue ink, appearing to read "Clayton Northouse".

Clayton Northouse
of LATHAM & WATKINS LLP



One Pickwick Plaza
Greenwich, Connecticut 06830
Tel: 203.618.5800 | 877.442.2757 | Fax: 203.618.7731
www.ibkr.com

41615*****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



May 16, 2024

Re: Notice of Data Breach. Please read this entire letter.

Dear Sample A. Sample:

Interactive Brokers LLC (the “Company”) writes to notify you of an incident that may affect the privacy of some of your information. Although we have no evidence of any identity theft or fraud, or any access to any client accounts, occurring as a result of this incident, this letter provides details of the incident, our response, and resources available to help you protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or around January 11, 2024, the Company identified a business email compromise that resulted in the unauthorized access to a limited amount of consumer personal information. Based on the Company’s subsequent investigation and forensic review, we determined the first activity relating to the business email compromise occurred on or around October 30, 2023. After detecting suspicious activity on January 11, 2024, the Company immediately activated its incident response protocols and implemented containment and remediation measures to ensure the security of the Company’s email environment.

What Information is Involved? Our investigation determined the following types of your information may have been impacted by this incident: your name and [Extra1]. At this time, we have no evidence that your information was subject to actual or attempted misuse as a result of this incident.

What Are We Doing? Data privacy and security are among the Company’s highest priorities, and we have extensive measures in place to help protect information in the Company’s care. We initiated a review of this incident and adopted immediate mitigation and remediation efforts, including resetting impacted employee account credentials. We also notified federal law enforcement. We are offering you complimentary credit monitoring services through Experian IdentityWorksSM for 24 months. We are also offering complimentary fraud detection tools through Experian’s IdentityWorks to help you monitor your personal information. Please see enrollment details below.

What You Can Do. It is always good practice to be vigilant by regularly reviewing your account statements and monitoring any available credit reports for suspicious activity. We also generally encourage you to take care in identifying calls, emails or SMS texts that appear to be spam or fraudulent (e.g., phishing), and to avoid opening links or attachments sent from untrusted sources. You may also review the section below on *Steps You Can Take to Help Protect Your Information* as a helpful resource.

For More Information. For further information, please call our Customer Service line at 1-877-442-2757 Monday to Friday from 8 am – 8 pm Eastern Time and Sunday from 1 pm – 7 pm Eastern Time.

Sincerely,

Interactive Brokers LLC

DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by July 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332, Monday through Friday from 8 am – 8 pm CST (excluding major U.S. holidays) by July 31, 2024. Be prepared to provide engagement number B121535 as proof of eligibility for the Identity Restoration services by Experian.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call toll-free 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file with the credit reporting bureau. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report free of charge, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	888-397-3742	800-680-7289
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover their information has been misused to file a complaint. You can obtain further information on how to file such a complaint using the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud (this letter alone does not suggest that you are a victim of or at risk of identity theft or fraud). Please note that in order for you to file a police report for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California residents, the California Office of Privacy Protection (www.oag.ca.gov/privacy) may be contacted for additional information on protection against identity theft. The California Attorney General can be contacted at 1300 I Street, Sacramento, CA 95814, www.oag.ca.gov, 800-952-5225.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 888-743-0023.

For North Carolina residents, the North Carolina Attorney General can be contacted at Mail Service Center 9001, Raleigh, NC 27699, www.ncdoj.gov, 877-566-7226.

For Rhode Island residents, the Rhode Island Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400. You have the right to file or obtain a police report regarding this incident.

For District of Columbia residents, the District of Columbia Attorney General can be contacted at 400 6th Street NW, Washington, DC 20001, www.oag.dc.gov, 202-727-3400.

For Iowa residents, the Iowa Attorney General can be contacted at 1305 E. Walnut Street, Des Moines, Iowa 50319, www.iowaattorneygeneral.gov, 515-281-5926, or 888-777-4590.

For New York residents, the New York Attorney General may be contacted at the Capital, Albany, NY 12224, www.ag.ny.gov, 800-771-7755.

For Oregon residents, the Oregon Attorney General may be reached at 1162 Court Street NE, Salem, OR 97301, www.doj.state.or.us, 503-378-6002.

For South Carolina residents, the South Carolina Department of Consumer Affairs may be reached at 293 Greystone Blvd., Ste. 400, Columbia, SC 29210, www.consumer.sc.gov, 800-922-1594.

For Kentucky residents, the Kentucky Attorney General may be contacted at 700 Capital Avenue, Suite 118, Frankfort, KY 40601, www.ag.ky.gov, 502-696-5300.

For New Mexico residents, you have the right to obtain a police report regarding 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. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

