



WESTEXEC ADVISORS

March 17, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To: Office of the Attorney General
Re: WestExec Advisors, LLC notification of potential data breach of third-party payment processing vendor

Dear Attorney General Brown,

On March 2, 2023, we were made aware that an unauthorized user may have gained access to the systems of a third-party payroll and payment processing vendor that WestExec Advisors uses, S Grover CPA. We are in the very early stages of working with the vendor to determine what exactly happened and what, if any, of our data may have been compromised, but out of a real abundance of caution, we are reporting this incident to the Maryland Attorney General's office, as well as sending notices to affected personnel.

This potential breach affected 14 Maryland Residents. Potential data compromised include Social Security Numbers, certain banking account numbers, addresses, and Tax ID information pertaining to current and former WestExec Advisors personnel.

What We Are Doing:

- We are working with the vendor to obtain more information and take steps to protect the information of our personnel.
- WestExec is no longer using this vendor to process any payments.
- No WestExec email or system was compromised as part of this incident
- We are providing 12 months of free credit monitoring to personnel who may have been affected by this potential breach.

Attached is the notice that we are providing to affected parties.

If you have additional questions, please contact me at 202-688-3346, rebecca@westexec.com, or WestExec Advisors, c/o Rebecca Skoryanc, Director of Operations, 875 15th St NW, Suite 550, Washington, DC 20005.

Sincerely,

Rebecca Skoryanc
Director of Operations



WESTEXEC ADVISORS

March 17, 2023

«First_Name» «Last_Name»

«Address»

«City», «State» «Zip»

Re: Notice of Data Incident

Dear «First_Name»,

We write to make you aware of a recent incident that we believe could have affected certain parts of your personal information.

What Happened? We were recently made aware that an unauthorized user may have gained access to the systems of a third-party payroll and payment processing vendor that WestExec Advisors uses. We are in the very early stages of working with the vendor to determine what exactly happened and what, if any, of our data may have been compromised, but out of a real abundance of caution, we want to let you know that the records entrusted to this vendor included personal information such as Social Security Numbers, certain banking account numbers, addresses, and Tax ID information pertaining to current and former WestExec personnel and may have been compromised as part of this incident.

What We Are Doing. Remediation efforts to mitigate any impact on our personnel are already underway and we no longer use this vendor to process any payments. We want to assure you that no WestExec email or system was compromised as part of this incident and that we are taking prompt action with the processing vendor to protect our personnel from any adverse impact.

We also are notifying you so that you may take further steps to protect your information, should you feel it appropriate to do so. In order to be proactive, we are also providing you with access to 12 months of credit monitoring and identity protection services at no charge to you.

What You Can Do. Please review the enclosed “*Steps You Can Take to Help Protect Your Information*” for further details, which describes the credit monitoring and identity protection services we are offering and how to activate them. We also encourage you to remain vigilant against the potential for identity theft and fraud and to monitor your credit reports for any potential suspicious activity.

For More Information. If you have additional questions, please contact me at 202-688-3346, rebecca@westexec.com, or WestExec Advisors, c/o Rebecca Skoryanc, Director of Operations, 875 15th St NW, Suite 550, Washington, DC 20005.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is very important to us, as we know it is to you.

Sincerely,

Rebecca Skoryanc
Director of Operations

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Complimentary Identity Monitoring Services

WestExec will reimburse you for one year of credit monitoring through LifeLock by Norton. You may select either the individual **Select** or **Advantage** program, choose annual payment, and sign up. Once you have done that, please send the full receipt to Rebecca@westexec.com and we will work with you to process a reimbursement.

<https://lifelock.norton.com/offers>

Note that the program automatically renews after one year, but you may cancel at any time. This is, of course, entirely optional, and if there is another company you prefer to use, please get in touch and we will be happy to coordinate that.

Monitor Your Accounts

We encourage you to remain vigilant against any potential incidents of identity theft and fraud and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. 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 bureaus listed below to request a free copy of your credit report. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

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 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.); and
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.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. 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 agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

[www.transunion.com/
fraud-alerts](http://www.transunion.com/fraud-alerts)

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

[www.equifax.com/personal/credit-
report-services](http://www.equifax.com/personal/credit-report-services)

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can 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 that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you experience identity theft or fraud. Please note that in order to file a report with law enforcement 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 Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-528-8662; or www.oag.state.md.us.

For District of Columbia residents, the Office of the District of Columbia Attorney General can be contacted at: 400 6th Street, NW, Washington, DC 20001; Phone (202) 727-3400; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: oag@dc.gov; or you may visit the website of the Office of the District of Columbia Attorney General at <https://dc.gov/agency/office-attorney-general-0>.

For North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.