



<Date>

[First name] [Last name]  
[Address]  
[City], [State] [Zip]

## Notice of Data Breach

Dear [Name],

As you may know, this spring the Democratic National Committee (DNC) discovered that it had been the victim of an illegal cyberattack by state-sponsored hackers. In July—on the eve of the Democratic National Convention—WikiLeaks posted to the Internet email messages (and attachments) that were stolen from the DNC. We are sending you this letter because the email messages posted by WikiLeaks contained your personal information. *Please carefully read this notice.*

### What Happened?

At the end of April 2016, the DNC discovered malicious computer software (“malware”) on its system and determined that it had been the victim of a computer intrusion. We immediately retained a leading cybersecurity firm, CrowdStrike, to assist in securing our network and determining the scope of the attack. CrowdStrike’s investigation identified two groups of state-sponsored hackers who had gained access to our network, one in the summer of 2015 and one in approximately April 2016. In June 2016, we completed repairs of our network and made a public statement concerning the intrusion. At the time, CrowdStrike found no evidence that email or documents containing personal information had been removed from our servers. However, on July 22, 2016, WikiLeaks publicly released a cache of approximately 20,000 emails that apparently had been stolen by the hackers. Some of those emails included personally identifiable information.

### What Information Was Involved?



## What We Are Doing

As described above, immediately after the DNC discovered malware on this system, we retained CrowdStrike to assist in securing our network and we continue to work with them and other security vendors as appropriate. We also are cooperating with federal law enforcement on its investigation of these intrusions.

To help protect you, we are also offering one year of credit monitoring, identity theft protection and fraud restoration services through ID Experts®. ID Experts' MyIDCare includes 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

You can enroll in these services by visiting [www.idexpertscorp.com/protect](http://www.idexpertscorp.com/protect) or by calling 866-329-9984.

*Please do not discard this letter; when enrolling, you will need to reference the following access code: <<Enrollment code>>.*

ID Experts is available Monday through Friday from 6 am - 6 pm Pacific Time. Please note that the deadline to enroll is November 18, 2016. If you are under age 18, you should not have a credit history established and therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. Your parent or guardian may enroll you into the services using the access code provided above.

## What You Can Do / More Information

We recommend that you take advantage of the protection offered by ID Experts. Please also review the enclosed information regarding identity theft and your credit report.

You may also contact us in writing at [breach\\_questions@dnc.org](mailto:breach_questions@dnc.org) or 430 South Capitol Street SE, Washington, D.C., 20003, or you can call us at 202-743-7484.

On behalf of the DNC, we regret any inconvenience this may cause you.

Sincerely,

Donna Brazile  
Interim Chair, Democratic National Committee



## **Additional Information Regarding Identity Theft and Your Credit Report**

The Federal Trade Commission (FTC) provides information about how to avoid identity theft and what to do if you suspect your identity has been stolen. You may contact the FTC at FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, [www.consumer.ftc.gov](http://www.consumer.ftc.gov), 1-877-ID-THEFT (877-438-4338). You can also contact local law enforcement or the attorney general's office in your state if you suspect that you have been the victim of identity theft.

You also may obtain a free copy of your credit report maintained by each of the three credit reporting agencies by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling toll-free 1-877-322-8228. Review the reports carefully, and if you find anything you do not understand or that is incorrect, contact the appropriate credit reporting agency.

You also may consider contacting the credit reporting agencies directly if you wish to put in place a fraud alert or a security freeze or to obtain additional information regarding identity theft. An initial fraud alert is free and lasts for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the credit company contact you prior to establishing any accounts in your name. In contrast, a security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without prior written permission. Placing a security freeze on your credit report may delay your ability to obtain credit.

To place a fraud alert or security freeze on your credit report, contact any the three credit reporting agencies using the contact information below:

- Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9554, Allen, TX 75013
- TransUnion: 1-800-916-8800; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19022-2000

*Additional information for Maryland residents:* You may contact your attorney general for additional information regarding identity theft at the Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023 or [www.oag.state.md.us](http://www.oag.state.md.us).