



Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789
By First Class Mail

September 27, 2017

NOTICE OF DATA BREACH

Dear John Sample,

I am writing to inform you that some of your personal information held by PerfectServe, Inc. ("PerfectServe") may have been compromised. At this time, we do not know for certain that PerfectServe's systems or vendors were the source of such compromise. However, out of an abundance of caution, PerfectServe is sending you this notification and is providing you with the opportunity to enroll in identity theft protection services, at no cost to you.

What Happened?

Beginning on August 28, 2017, PerfectServe began to receive reports that employees had been receiving letters from the IRS containing transcripts of their recent tax filings. These individuals informed PerfectServe that they had not requested these documents. While at present, we do not know that PerfectServe or any of its vendors is the source of this apparent compromise of data, we have nonetheless made the determination to inform you of the situation.

What Information Was Involved?

Based on the information that we understand is necessary to obtain the IRS documents in question, it appears that names, dates of birth, addresses, and social security numbers for certain employees and former employees, and in some cases spouses and children, may have been compromised. For spouses or children whose information we believe may have been impacted, we have sent separate notice letters to them to the address we have on file.

What We Are Doing.

PerfectServe is diligently working to investigate this matter, and we have engaged a nationally-known cybersecurity firm to perform forensic analyses on our systems. This investigation is ongoing. PerfectServe has also notified law enforcement and the IRS about this incident, and is cooperating with these authorities in the handling and investigation of this matter. PerfectServe will continue to take security measures designed to safeguard its systems against potential breaches.

As an added precaution, we have arranged to have AllClear ID protect your identity for 3 years at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 3 years.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-422-7206 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.



01-04-1-00

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-422-7206 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

What You Can Do.

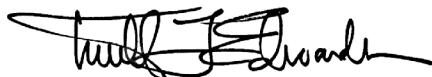
In addition to taking advantage of the identity protection services above, please see the attached "Additional Actions To Help Reduce Your Chances of Identity Theft" which is part of this notice, for further information on actions you can take to protect against identity theft. In addition, the IRS has suggested that you consult its resources regarding identity theft, which we have attached.

For More Information.

We take the protection of your personal information seriously. As discussed above, we are working with law enforcement and tax authorities, and have retained the services of a cybersecurity forensics firm to assist us in investigating and remediating this incident.

If you have further questions or concerns about this incident, you can contact AllClear ID at 1-855-422-7206, Monday through Saturday, 8:00 a.m. – 8:00 p.m. Central Time. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

A handwritten signature in black ink, appearing to read "Terry Edwards". The signature is fluid and cursive, with a long horizontal stroke extending to the left.

Terry Edwards
President & CEO

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit www.annualcreditreport.com or call (877) 322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➤ **USE TOOLS FROM CREDIT PROVIDERS**

We recommend you remain vigilant for instances of fraud and identity theft. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➤ **PLACE A FRAUD ALERT ON YOUR CREDIT FILE**

There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. An **initial fraud alert** stays on your credit report for at least 90 days, while an **extended fraud alert** stays on your credit report for seven years and may be placed on your credit report if you have already been a victim of identity theft and have the appropriate documentary proof. A fraud alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud or identity theft. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax
(888) 766-0008
www.equifax.com

Experian
(888) 397-3742
www.experian.com

TransUnion
(888) 909-8872
www.transunion.com

➤ **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. **Security freezes must be placed separately for each of the credit reporting companies**, who may charge a fee to place, temporarily lift, or permanently remove a security freeze. Such fees may vary from state to state.

To place a security freeze on your credit report, you must send a separate request to **each** of the three major consumer credit reporting agencies (Equifax, Experian, and TransUnion) online, by telephone, or by regular, certified, or overnight mail as provided below:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
(800) 685-1111 (For NY Residents: (800) 349-9960)
<https://www.freeze.equifax.com/>

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
(888) 397-3742
<https://www.experian.com/freeze/center.html>

TransUnion Security Freeze

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
(888) 909-8800
<https://www.transunion.com/credit-freeze/place-credit-freeze>



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 (5) 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; or
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies through their websites, via telephone, or by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must contact each of the three credit bureaus through their websites, by telephone (where permitted), or by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

➤ **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of with whom you are sharing your personal information; and shredding receipts, statements, and other sensitive information.

➤ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

You may obtain more information from the Federal Trade Commission (FTC) about steps you can take to avoid identity theft, including how to place a fraud alert or security freeze on your credit file. The FTC may be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580.
ID Theft hotline: (877) IDTHEFT (438-4338)
www.ftc.gov
www.identitytheft.gov

➤ **REDUCE THE RISK OF TAX-RELATED FRAUD**

To reduce the risk of tax-related fraud, you may contact the IRS Identity Protection Specialized Unit at (800) 908-4490 (Monday through Friday, 7:00 am – 7:00 pm local time). The IRS also provides identity theft-related resources at <https://www.irs.gov/identity-theft-fraud-scams/identity-protection>. You may also want to contact your state tax authority and tax advisors to notify them of the potential for identity theft and to protect against the possibility of a fraudulent tax return.

➤ **RESIDENTS OF MARYLAND**

Maryland residents can obtain information from the Maryland Attorney General about steps they can take to avoid identity theft at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
Consumer@oag.state.md.us
www.oag.state.md.us

➤ **RESIDENTS OF MASSACHUSETTS**

Under Massachusetts law, you have a right to obtain any police report filed in regard to 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.

Massachusetts law also allows consumers to place a security freeze on their credit reports. See above for details on security freezes, including how to place, temporarily lift, or permanently remove a security freeze on a credit report. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, that credit reporting agency cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

➤ **RESIDENTS OF NORTH CAROLINA**

North Carolina residents can obtain information from the North Carolina Attorney General about steps they can take to avoid identity theft at:

North Carolina Office of the Attorney General

9001 Mail Service Center

Raleigh, NC 27699

(877) 566-7226 (toll-free in North Carolina)

(919) 716-6400

www.ncdoj.gov/Consumer.aspx



AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 36 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 36 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”);
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------



04-04-1