

**March 6, 2017**

## **NOTICE OF DATA BREACH**

Dear Valued Employee:

We are contacting you about a data breach that has occurred at NSC Technologies, LLC.

### What Happened?

On March 2, 2017 an on-line hacker posing as NSC's CEO emailed the company's payroll department and directed that copies of employee W-2 forms be sent to him. Believing the request to come from the CEO, the payroll department forwarded PDF copies of a number of employee IRS W-2 forms to the requestor, who was using a false email address that appeared to belong to NSC's CEO. Although this "spoofing" episode was identified for what it was literally moments after the W-2 forms were sent to the hacker, by that point the forms themselves had already been shared with him or her. At this point we have no indication that any of the information contained on the W-2 forms that the payroll department was tricked into sharing with the hacker has been misused in any way, but the potential for such misuse certainly exists.

### What Information Was Involved?

This incident involved your 2016 IRS W-2 form, which includes your name, address, social security number, and 2016 income and withholding information.

### What Are We Doing?

We have notified appropriate federal, state, and local law enforcement agencies of this theft of employee data, as well as alerting both the Federal Trade Commission and the federal Internal Revenue Service of this data breach. We have also advised credit reporting companies Equifax, Experian, and TransUnion of this incident. Additionally, we are providing you with one year of free Identity Force identity theft protection and credit monitoring services, at no cost to you, as this service is being paid for by NSC.

This notification has not been delayed as a result of any law enforcement investigation into this incident.

### What Can You Do?

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus (Equifax, Experian, and TransUnion). As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days.

**THE  
STAFFING  
EXPERTS**

**Safety - Quality - Integrity - Flexibility - Accountability**  
*"Together we build a stronger America."*

500 Crawford Street, Suite 401, Portsmouth, VA 23704 | 866.672.2677 | [www.nsc-tech.com](http://www.nsc-tech.com)

Equifax: Equifax.com or 1-800-525-6285  
Experian: Experian.com or 1-888-397-3742  
TransUnion: transunion.com or 1-800-680-7289

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report and get a copy of the police report; you may need it to clear up any fraudulent debts.

If your personal information has been misused, visit the FTC's site at [IdentityTheft.gov](http://IdentityTheft.gov) to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You may also want to consider contacting the major credit bureaus at the telephone numbers above to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at [naag.org](http://naag.org) to learn more.

You can go to [IdentityTheft.gov](http://IdentityTheft.gov) about steps you can take to help protect yourself from identity theft, depending on the type of information exposed.

To activate your one year of free identity theft protection and credit monitoring services at no cost to you, please call NSC's Escalation Hotline at 757-274-8658 to be provided a Verification Code. Once you have your Verification Code, you can then enroll with Identity Force using its secure web site. To sign up on-line for this free service, please visit: <https://secure.identityforce.com/benefit/XXXX> and follow the on-screen instructions that will guide you through the enrollment process. You will need your Verification Code to activate this service. You must complete the enrollment process online to take advantage of the identity theft protection services we are offering you. By law, we cannot do this on your behalf. Should you need further assistance with this process, in addition to calling NSC's Escalation Hotline, you can also contact Identity Force's Membership Services at 1-877-694-3367, Monday through Friday from 8:30 AM to 5:30 PM, Eastern Time.



Other Important Information

You may want to consult “Breach Help—Consumer Tips from the California Attorney General”, which you can obtain in downloadable PDF form on the California Attorney General’s website, at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf>.

And for even more information on identity theft, you may visit the web site of the California Department of Justice, Privacy Enforcement and Protection at [www.privacy.ca.gov](http://www.privacy.ca.gov).

Call This Number or Go to This Website for More Information

You can call 757-274-8658 for more information. If and when additional information is known that may be of assistance to you in connection with this data breach, we will provide it to you via updates to your email and postal addresses as well as posting it on the company website: [www.nsc-tech.com](http://www.nsc-tech.com).

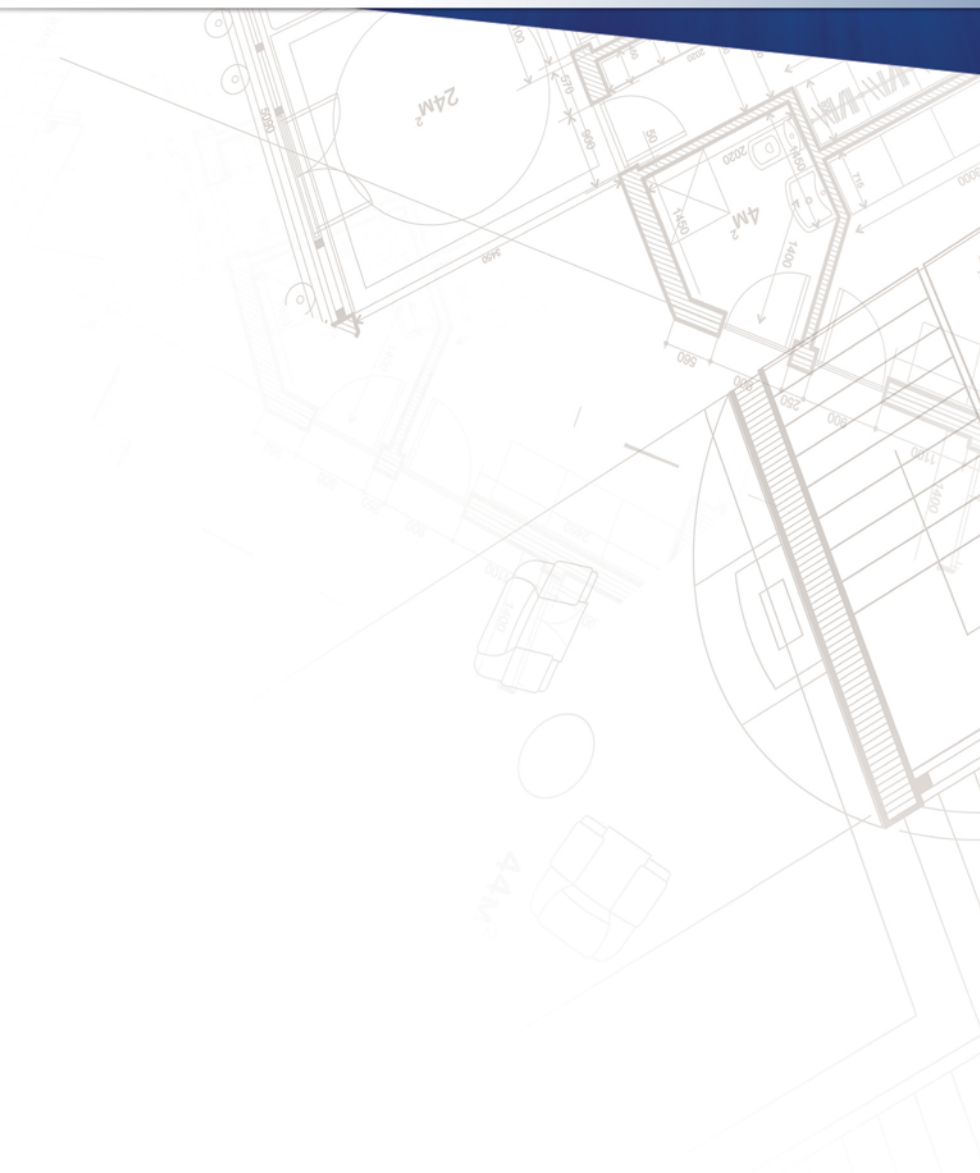
Needless to say, we are quite disappointed that this incident occurred and NSC deeply regrets any inconvenience or difficulty it may cause you. I can assure you that we are doing everything in our power to make sure that something like this does not happen again.

Sincerely,

*Paul Rodriguez*  
Paul Rodriguez, CEO

THE  
**STAFFING**  
EXPERTS

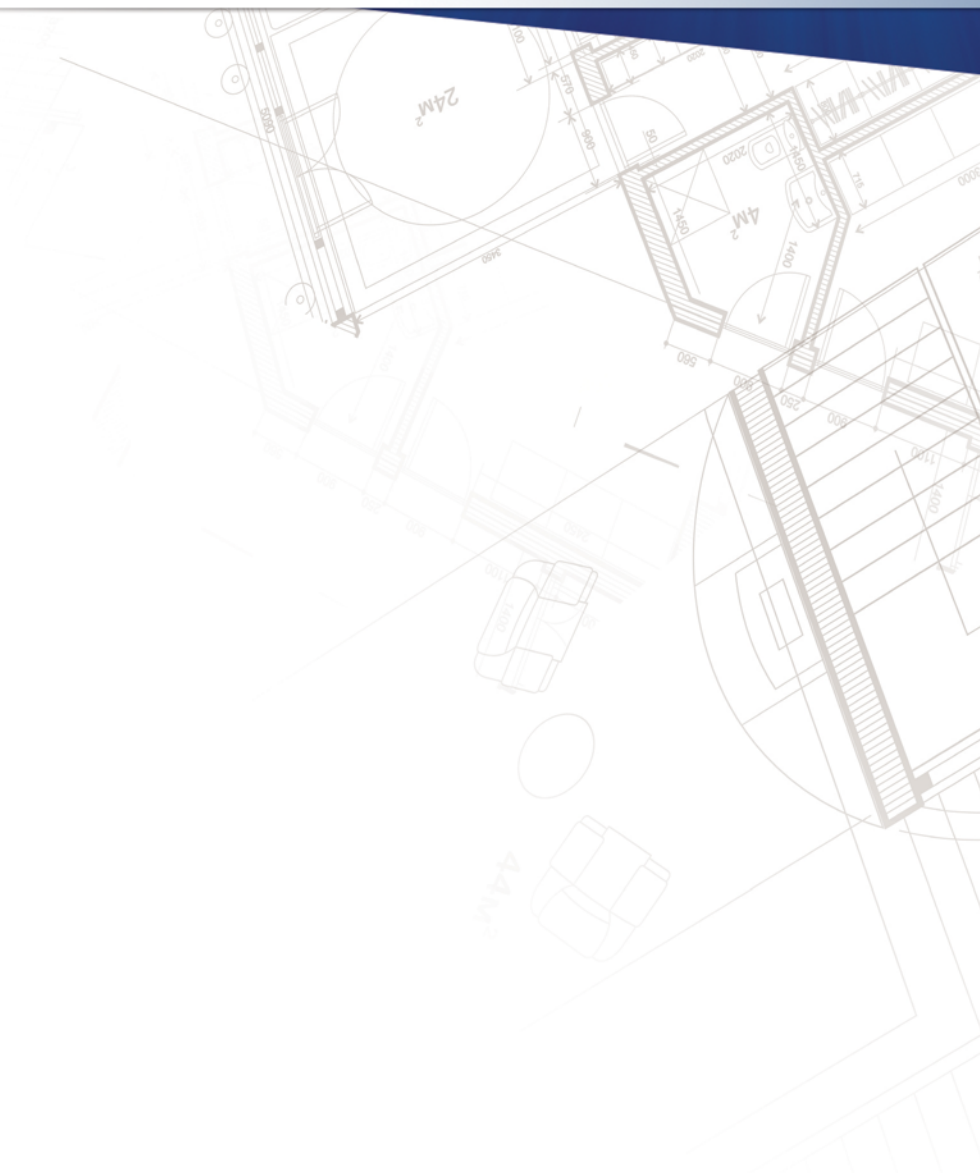
Safety - Quality - Integrity - Flexibility - Accountability  
"Together we build a stronger America."



# THE STAFFING EXPERTS

Safety - Quality - Integrity - Flexibility - Accountability  
*"Together we build a stronger America."*

500 Crawford Street, Suite 401, Portsmouth, VA 23704 | 866.672.2677 | [www.nsc-tech.com](http://www.nsc-tech.com)



# THE STAFFING EXPERTS

Safety - Quality - Integrity - Flexibility - Accountability  
*"Together we build a stronger America."*

500 Crawford Street, Suite 401, Portsmouth, VA 23704 | 866.672.2677 | [www.nsc-tech.com](http://www.nsc-tech.com)