

BRUNSWICK

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



00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 6, 2016

Subject: Notice of Brunswick Employee Data Incident. After reading this entire letter, if you have any questions, please contact 1-855-904-5763.

Dear John Sample:

As a current or former employee of Brunswick Corporation (“Brunswick”), you entrust us with certain personal information that is required for a number of administrative purposes, including processing your payroll and taxes. Regrettably, we are writing to inform you that a file containing some of your personal information was mistakenly transmitted to an unauthorized recipient. We want to make sure you are fully informed of the situation, what we are doing to help, and steps you can take to further protect your personal information.

What Happened?

On April 29, 2016, a file containing the IRS Form W-2 for a number of Brunswick employees was mistakenly transmitted to an unauthorized recipient. An employee received an email from a cyber attacker posing as a Brunswick executive requesting the W-2 information. The employee, not realizing that the email was from an impersonator, provided the requested information. Unfortunately, this file included your W-2 form. The employee who mistakenly transmitted the file to the unauthorized recipient informed management upon realizing what had happened.

If you did not receive a W-2 from Brunswick for 2015, you are not affected by this incident.

In light of this incident, we are reviewing our security policies and employee training procedures.

What Information Was Involved?

The information included your name, address, Social Security number, income, and 2015 tax information. Only information contained in your W-2 form was transmitted.

What We Are Doing.

Brunswick has arranged to have **AllClear ID** protect your identity for 24 months at no cost to you. The following identity protection services have been in place since the date of the incident, and you can use them at any time during the next 24 months. You can find out more about AllClear ID at www.allclearid.com.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem



arises, simply call 1-855-904-5763 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO 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 1-855-904-5763 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.

Additional details on these services are included at the end of this letter. **Please retain this information; you will need it to register for services.** You will not need to provide a credit card or sign up for any other service provided by AllClear ID in order to access this product.

What You Can Do.

As a precautionary measure, there are a number of additional steps you can take to protect yourself, such as placing a fraud alert on your credit report or contacting the appropriate authorities if you believe you have been the victim of identity theft. The enclosed "Identity Theft Protection Tips" describes some of these steps. Of course, it is always important that you remain vigilant by periodically reviewing your financial account statements and credit reports for signs of fraud.

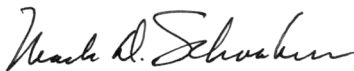
Other Important Information.

If you believe you are the victim of identity theft, you should contact your local law enforcement and file a police report. For additional information, view the enclosed "Identity Theft Protection Tips."

For More Information.

We deeply regret this incident and are committed to ensuring that your personal information remains protected. If you have any questions, please call Brunswick at 1-888-735-4767 for questions about fraud, identity theft, or the AllClear ID services.

Sincerely,



Mark D. Schwabero
Chairman and Chief Executive Officer

IDENTITY THEFT PROTECTION TIPS

You should consider taking the following steps to further protect yourself and your identity:

Enroll in the AllClear ID services. As explained above, Brunswick has arranged to have AllClear ID protect your identity for 24 months at no cost to you. See the information within the letter, above, regarding how to enroll. Please note that the Redemption Code provided is specific to you and should not be shared with anyone. Please note also that only you can activate your membership. We cannot activate this product on your behalf.

Vigilantly monitor your credit files, bank account statements, credit card statements, etc. closely for indications of identity theft or other misuse. We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Place a fraud alert on credit files. A fraud alert notifies lenders that you may be the victim of identity theft and requires them to take certain verification procedures before opening new accounts in your name. There are also 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. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Credit Freezes (for Non-Massachusetts Residents): Place a credit freeze on credit files. State laws permit you to place a credit freeze, also known as a security freeze, on your credit file. The purpose of a freeze is to prevent credit cards, loans, or other forms of credit from being opened in your name without your permission by restricting access to your credit report. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state.

Depending on the applicable state laws, there may be a small charge for placing a freeze on your credit file. **Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.** Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

For more information about placing a security freeze or fraud alert on your credit file, contact the following credit reporting agencies:



Equifax
PO Box 105788
Atlanta, GA 30348
www.equifax.com
888-766-0008

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com
800-680-7289

If you believe you are the victim of identity theft, you should contact your local law enforcement and file a police report. You should also consider contacting the U.S. Federal Trade Commission's identity theft hotline at (877) 438-4338, or www.ftc.gov/idtheft to file a report and to obtain more information about combating identity theft. You may also wish to contact your state Attorney General. Maryland residents can contact their AG at: (410) 576-6566; North Carolina residents can contact their AG at: (919) 716-6000; contact information for the other Attorneys General is available at: <http://www.naag.org/current-attorneys-general.php>. The FTC and your state Attorney General can also provide you with additional information on how to protect yourself from identity theft.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

AllClear Secure 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:

- Twenty-four (24) months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by Brunswick.

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 Secure 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 24 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements

To be eligible for Services under AllClear Secure 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 Secure 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 Secure 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;
- 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 Secure 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
- 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;

In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure 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 Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and 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 Secure 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 Secure, please contact AllClear ID:

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

SUPPORT INFORMATION
BRUNSWICK DATA FREQUENTLY ASKED QUESTIONS

What happened?

On April 29, 2016, a file containing the IRS Form W-2 for a number of Brunswick employees was mistakenly transmitted to an unauthorized recipient. An employee in the payroll department received an email address from a cyber attacker posing as a Brunswick executive, requesting the W-2 information. The employee, not realizing that the email was from an impersonator, provided the requested information. Unfortunately, this file included your W-2 form. The employee who mistakenly transmitted the file to the unauthorized recipient informed management upon realizing what had happened.

If you did not receive a W-2 from Brunswick for 2015, you are likely not affected by this incident.

In light of this incident, we are reviewing our security policies and employee training procedures.

Brunswick is providing credit monitoring and reporting, identity theft assistance services, and identity theft insurance for every affected individual. Please note that we cannot enroll you in the services. You must register yourself. In the meantime, you may want to consider taking some additional steps to protect against identity theft and fraud, such as reviewing a free copy of your credit report or placing a fraud alert or credit freeze on your credit file.

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

You may obtain additional information about placing a fraud alert or credit freeze on your credit file by contacting one of the credit reporting agencies:

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

What information was compromised/accessed/acquired? Should I be worried about fraud or identity theft?

W-2 forms contain your name, address, Social Security number, income, and all taxes withheld.

Law enforcement agencies have indicated that fraud from identity theft can happen very quickly and that W-2s, in particular, have become a major target of cyber attackers. You should remain vigilant by reviewing your financial account statements and credit reports for signs of fraud.

Was my spouse or other family members' information also affected?

No, family members' information was not affected.

Was there additional information that was compromised – for example, bank accounts?

No, bank account numbers were not exposed, only the information contained on your W-2 form. However, as a precaution, you may want to inform your banks and other financial institutions that your personal information was compromised.

When did this happen? How did Brunswick discover that it happened?

The file was sent on Friday, April 29, 2016. The employee who mistakenly transmitted the file to the unauthorized recipient informed management immediately, upon realizing what had happened.



What is Brunswick doing to address the incident and protect me from fraud or identity theft?

We are reviewing our security policies and employee training procedures. We are offering you 24 months of complimentary credit monitoring and reporting, identity theft assistance services, and identity theft insurance for every affected employee. Please note that we cannot enroll you in the services, you must register yourself.

The protection you will receive from the service is already in place and an identity repair service is available even if you opt not to enroll in the full range of services. If you identify that you have been the victim of fraud or identity theft, AllClear ID will be able to help you investigate and resolve the situation.

Brunswick realizes that dealing with these issues can be time-consuming and frustrating. In the unfortunate event that you need to resolve any fraud or identity theft issues, please take the reasonable time necessary to address the situation during your normal work hours.

What should I be doing to protect myself?

You should enroll in the complimentary credit monitoring and remain vigilant for suspicious emails or activity on your credit card, bank, and other financial statements. You should be cautious and refrain from clicking on links or attachments in emails from unknown senders.

You may want to consider taking some additional steps to protect against identity theft and fraud, such as reviewing a free copy of your credit report or placing a fraud alert or credit freeze on your credit file.

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: There are also 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. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Equifax
PO Box 105788
Atlanta, GA 30348
www.equifax.com
888-766-0008

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com
800-680-7289

If you believe you have been the victim of fraud or identity theft you should contact your local law enforcement and file a police report.

How long should we monitor our credit?

There is no “expiration date” on stolen information, so it is a good idea to review credit reports, bank, credit card and other account statements regularly. Proactively create alerts on credit card and bank accounts for suspicious activity. If unauthorized or suspicious activity is discovered, do not delay! Take action immediately.

What is Brunswick doing to protect my information moving forward?

Brunswick has a strong commitment to privacy and data. We are committed to reviewing and improving our security policies, procedures, and training moving forward.

Have you notified the police or law enforcement? Has the person who received the information been caught?

The matter has been reported to the IRS and to the appropriate law enforcement authorities and government entities in accordance with applicable law. We do not know at this time who the cyber attacker is, or whether she or he has been caught.

Do I need to do anything regarding my taxes or contact the IRS?

Because your W-2 was affected, someone could file a fraudulent tax return using your Social Security number now or in the future. You should obtain from the IRS an Electronic Filing PIN. The PIN may not protect your 2015 return, but it will provide protection for future filings.

Visit <http://www.irs.gov/Individuals/Electronic-Filing-PIN-Request> or call 866-704-7388 and follow the system prompts. If an accountant or tax preparer files your return on your behalf, he or she may have a PIN for you. Be sure to discuss this incident with your tax preparer.

If you haven't filed taxes for 2015 and no other return has been submitted in your name, the IRS recommends you file your taxes electronically, even if your data is not complete or it contains errors. You can correct any errors in that return with an amended filing at a later date. Filing an electronic return quickly prevents someone else (who wants to misuse your information) from taking your allocated “slot” in the IRS e-file system.

If you have filed for 2015, you can still submit an IRS Form 14039, Identity Theft Affidavit, in order to protect yourself in the future. If a fraudulent return has been electronically filed in your name, you must:

File a paper tax return with a completed IRS Form 14039, Identity Theft Affidavit. The IRS recommends that you attach that form to the front of the paper return.

The IRS has indicated that it may take up to six months to process the valid tax return you filed after a fraudulent return was also filed.

Will we receive any additional information or update?

We will continue to communicate with you as appropriate regarding this situation.



Why didn't you alert me sooner?

We worked to notify people and include a recommended response plan once we confirmed what was released and which people were impacted. Further, we notified employees on their first day back at work following being notified and confirming the data incident.

I'm in the midst of refinancing / buying a home / buying a car, what should I do?

Explain the issue to your bank or financing company, and check your credit report for suspicious activity.

What happens if my credit is compromised?

If you identify that you have been the victim of fraud or identity theft, AllClear ID will be able to help you investigate and resolve the situation.