September 1, 2017

Re: Bright Wood Security Breach Notification

Bright Wood®
1960 - 2010 50 Years of Quality Millwork

Name

Dear Name:

We are contacting you because Bright Wood Corporation recently experienced a series of potential data security breaches involving the personal information of some of our current and former employees. We are writing to provide you with information about the incident and steps you can take to protect yourself. We truly regret that this incident occurred and any inconvenience it may cause you.

What Happened

We recently learned that an unauthorized third party breached the Bright Wood network and may have accessed data files stored on our system containing records of current and former employees.

What Information Was Involved

We believe that certain employee information, including names, addresses, birth dates and social security numbers may have been accessed. Please be assured that personal banking information is not stored on our systems and was not subject to this incident.

What We Are Doing

After becoming aware of the system beach, Bright Wood implemented additional security measures designed to prevent the recurrence of such an attack including, without limitation, changing administrative passwords, rebuilding servers, and updating firmware where appropriate. In addition, we are identifying and deploying further security measures to reduce the risk of a reoccurring breach. We are actively working with law enforcement and will continue to cooperate in their investigation of the incident. We also have notified the three major U.S. credit reporting agencies about this incident and have given those agencies a general report, alerting them to the fact that the incident occurred.

In an effort to help protect you from the potential misuse of your information, we have retained Experian, a specialist in identity theft protection, to provide you with one year of identity monitoring services (IdentityWorks) at no charge to you. Experian IdentityWorks helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. Included with this service are fraud resolution services that provide a Fraud Resolution Agent to work with you to investigate and resolve incidents of fraud that occurred after the data breach. The Fraud Resolution assistance is immediately available to you without any further action on your part; you simply need to call 1-877-890-9332 to report an incident and speak with a Fraud Resolution Agent. Additionally, you can activate the fraud detection tools available through enrolling in IdentityWorks, also at no cost to you. To enroll in the services, visit https://www.experianidworks.com/creditone by November 30, 2017 and use the following activation code: XXXXXXX. You may also enroll over the phone by calling 1-877-890-9332. Be prepared to provide engagement number XXXXXX as proof of eligibility for these services.

What You Can Do

The Federal Trade Commission suggests the following steps:

1. 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. 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.
    - Equifax: www.equifax.com or 1-800-525-6285
    - Experian: www.experian.com or 1-888-397-3742
    - TransUnion: www.transunion.com or 1-800-680-7289
2. Request that all three credit reports be sent to you, free of charge, for your review. Carefully review your credit reports. Look for inquiries from companies that you haven't contacted, accounts that you did not open and debts on your accounts that you can't explain. Be aware that some companies may bill under names other than their store names. Close any accounts you know, or suspect, have been tampered with or opened fraudulently. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report. Get a copy of the police report; you may need it to clear up the fraudulent debts.
3. If your personal information has been misused, visit the FTC's site at 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.
4. Consider placing a credit freeze on your credit file so that no new credit can be opened in your name without a PIN number or other identity verification that is issued to you when you initiate a freeze. 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. You must contact each credit reporting agency mentioned above to place a credit freeze. The fees associated with placing a credit freeze differ from state to state so you will need to contact the three credit reporting agencies to find out more information.
5. Visit https://www.identitytheft.gov/ to report identity theft and get a recovery plan.

For More Information

If you have questions, please call 1-541-475-7799, Monday through Friday (excluding holidays) from 7:30 a.m. to 4:30 p.m. Pacific time or send an e-mail to: databreach@brightwood.com. Again, we sincerely regret any difficulty or inconvenience this incident may cause you.

Sincerely,

Dallas L Stovall

President/CEO

September 1, 2017

Asunto: Aviso de violación de seguridad de Bright Wood

Estimado(a): Name

Nos estamos poniendo en contacto con usted porque Bright Wood Corporation ha experimentado recientemente una serie de posibles infracciones de seguridad de datos que involucran la información personal de algunos de nuestros empleados actuales y anteriores. Estamos escribiendo para proporcionarle información sobre el incidente y los pasos que puede tomar para protegerse. Realmente lamentamos que este incidente haya ocurrido y cualquier inconveniente que pueda causarle.

¿Que pasó?
Recientemente nos enteramos de que un tercero no autorizado violó la red de Bright Wood y puede haber accedido a los archivos de datos almacenados en nuestro sistema que contienen registros de empleados actuales y antiguos.

¿Qué información estaba involucrada?
Creemos que puedo haber tenido acceso a cierta información de los empleados, incluyendo nombres, direcciones, fechas de nacimiento y números de seguridad social. Tenga la seguridad de que la información bancaria personal no está almacenada en nuestros sistemas y no está sujeta a este incidente

¿Qué estamos haciendo?
Después de tomar conocimiento de la violación del sistema, Bright Wood implementó medidas de seguridad adicionales diseñadas para evitar la repetición de un ataque, incluyendo, sin limitación, cambiar contraseñas administrativas, reconstruir servidores y actualizar el firmware cuando sea apropiado. Además, estamos identificando y desplegando nuevas medidas de seguridad para reducir el riesgo de una violación recurrente. Estamos trabajando activamente con la policía y continuaremos cooperando en su investigación del incidente. También hemos notificado a las tres principales agencias de informes crediticios estadounidenses sobre este incidente y les hemos dado un informe general, alertándolos de que el incidente ocurrió.

En un esfuerzo por ayudarle a protegerse del potencial mal uso de su información, hemos contratado a Experian, un especialista en protección contra robo de identidad, para proporcionarle un año de servicios de monitoreo de identidad (IdentityWorks) sin costo alguno para usted. Experian IdentityWorks ayuda a detectar el posible uso indebido de su información personal y le proporciona un soporte de protección de identidad centrado en la identificación inmediata y la resolución del robo de identidad. Se incluyen con este servicio servicios de resolución de fraude que proporcionan un agente de resolución de fraude para trabajar con usted para investigar y resolver incidentes de fraude que se produjeron después de la violación de datos. La asistencia para la resolución de fraude está inmediatamente disponible para usted sin ninguna otra acción de su parte; simplemente tiene que llamar al 1-877-890-9332 para reportar un incidente y hablar con un agente de resolución de fraude. Además, puede activar las herramientas de detección de fraude disponibles mediante la inscripción en IdentityWorks, también sin costo para usted. Para inscribirse en los servicios, visite https://www.experianidworks.com/creditone para November 30, 2017 y use el siguiente código de activación: XXXXXXX. También puede inscribirse por teléfono llamando al 1-877-890-9332. Esté preparado para proporcionar el número de compromiso XXXXXX como prueba de elegibilidad para estos servicios.

Que puede hacer:
La Comisión Federal de Comercio sugiere los siguientes pasos:

1. Ponga una alerta de fraude en su archivo de crédito. Una alerta de fraude le dice a los acreedores que se pongan en contacto con usted antes de abrir cualquier nueva cuenta o cambiar sus cuentas existentes. Llame a cualquiera de las tres principales agencias de crédito. Tan pronto como una oficina de crédito confirma su alerta de fraude, los otros son notificados para colocar alertas de fraude. La alerta de fraude inicial permanece en su informe de crédito durante 90 días. Puede renovarlo después de 90 días
    - Equifax: www.equifax.com o 1-800-525-6285
    - Experian: www.experian.com o 1-888-397-3742
    - TransUnion: www.transunion.com o 1-800-680-7289

2. Solicite que los tres informes de crédito le sean enviados gratuitamente para su revisión. Revise cuidadosamente sus informes de crédito. Busque consultas de empresas que no haya contactado, cuentas que no abrieron y deudas en sus cuentas que no puede explicar. Tenga en cuenta que algunas compañías pueden facturar bajo nombres distintos de los nombres de sus tiendas. Cierre cualquier cuenta que usted conozca o sospeche, haya sido manipulada o abierta fraudulentamente. Si encuentra actividad sospechosa en sus informes de crédito o tiene razones para creer que su información está siendo mal utilizada, presente un reporte policial. Obtenga una copia del informe de la policía; usted puede necesitarlo para aclarar las deudas fraudulentas

3. Si su información personal ha sido mal utilizada, visite el sitio de la FTC en IdentityTheft.gov para obtener los pasos de recuperación y para presentar una queja de robo de identidad. Su queja será agregada a la Red de Centinela del Consumidor de la FTC, donde será accesible a los encargados de hacer cumplir la ley para sus investigaciones.

4. Considere colocar un congelamiento de crédito en su archivo de crédito para que no se pueda abrir un nuevo crédito a su nombre sin un número de PIN u otra verificación de identidad que se le otorgue cuando inicie una congelación. Si coloca un crédito congelado, los posibles acreedores y otros terceros no podrán obtener acceso a su informe de crédito a menos que levante temporalmente la congelación. Por lo tanto, el uso de un congelamiento de crédito puede retrasar su capacidad para obtener crédito. Debe ponerse en contacto con cada agencia de informes de crédito mencionada anteriormente para establecer un congelamiento de crédito. Las tarifas asociadas con la colocación de una congelación de crédito difieren de estado a estado por lo que tendrá que ponerse en contacto con las tres agencias de informes de crédito para obtener más información.

5. Visite https://www.identitytheft.gov/ para reportar el robo de identidad y obtener un plan de recuperación.

Para más información
Si tiene preguntas, por favor llame al 1-541-475-7799, de luneas a viernes (excepto días festivos) de 7:30 a.m. a 4:30 p.m. tiempo Pacífico o envíe un correo electrónico a: databreach@brightwood.com. Una vez más, lamentamos sinceramente cualquier dificultad o inconveniente que este incidente pueda causarle.

Sinceramente,

Dallas L Stovall

Dallas Stovall
Presidente/CEO