



Freeman
Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009
www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

March 12, 2024

Via Email Only

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: IDtheft@oag.state.md.us

Re: Gamewell Mechanical, LLC – Notice of Data Event

Dear Sir or Madam:

We represent Gamewell Mechanical, LLC (“GMI”), a mechanical contracting company based in Salisbury, North Carolina. This letter is being provided pursuant to the Maryland Personal Information Protection Act, MD. CODE ANN. COM. LAW § 14-3501, et seq, which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of Maryland.

GMI recently learned of suspicious activity involving a company email account. GMI immediately commenced an investigation into the nature and scope of the incident. On or about January 19, 2024, GMI confirmed unauthorized access to an employee account by someone outside of the organization at various times between December 6, 2023, and January 17, 2024. GMI thereafter conducted further analysis of the impacted account for sensitive information and is notifying those individuals potentially impacted. The data points impacted include name, driver’s license number, and date of birth.

On March 12, 2024, GMI began providing notice to the potentially affected Maryland residents by U.S. regular mail. GMI is providing this notification to two (2) residents of the State of Maryland. A sample copy of the notice letter is attached here as Exhibit A.

GMI is providing written notice of the event that includes a brief description of the incident, encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements and credit reports, immediately reporting errors or suspicious

activity to the financial institution or service provider, and filing a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered, from any source. GMI enclosed documentation containing contact information for the major consumer reporting bureaus, the FTC, and state-specific regulators, a telephone number for the business that the person may call for further information and assistance, and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so. GMI is offering potentially impacted individuals twelve (12) months of identity theft monitoring and restoration services through IDX. The monitoring services include single bureau daily credit reporting, dark web monitoring through Cyberscan, fully managed ID theft recovery services and \$1 million identity theft insurance with no deductible.

After discovering the incident, GMI partnered with computer forensic specialists to investigate the incident to understand its nature and scope and reset the password to the email account. GMI continues to require multifactor authentication to company email accounts for all users. GMI will continue to review its policies and procedures for ways to enhance the existing protections it has in place to adapt to evolving threats. GMI is also notifying other state regulators as required.

I believe this provides you with all information necessary for your purposes and to comply with Maryland law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

/s/ Nicholas Jajko

Nicholas Jajko

Exhibit “A”



March 12, 2024

[REDACTED]
[REDACTED]
[REDACTED]

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code:

[REDACTED]

Re: Notice of Data Privacy Incident

Dear [REDACTED]:

Gamewell Mechanical LLC takes the security and privacy of personal data seriously. As part of that commitment, we are notifying you of a recent incident that could have involved your personal information. Please read this letter carefully.

What Happened?

Gamewell was recently notified of suspicious email activity involving a company email account. Consistent with our procedures, we commenced an immediate investigation into the activity that included partnering with computer forensic specialists to understand the nature and scope of the incident. On January 19, 2024, we confirmed unauthorized access to an employee email account at various times between December 6, 2023, and January 17, 2024, by someone outside our organization. We conducted further analysis of the impacted account and determined your sensitive personal information was present within the account and potentially subject to unauthorized access. While we have no evidence your information was taken or misused, we are notifying you out of an abundance of caution.

What Information Was Involved?

You are receiving this letter because our review confirmed your name, driver's license number, and date of birth were accessible to an unknown individual. We stress that we have no indication that any information was taken from the email account or misused but we are notifying you so that you may take advantage of the resources we are offering you, should you find it appropriate to do so.

What We Are Doing.

In addition to partnering with computer forensic specialists to investigate the incident to understand its nature and scope, we continue to require multi-factor authentication to company email accounts for all users. We are notifying the potentially impacted individuals of this incident out of an abundance of caution and are providing you with resources you may take advantage of to protect your information. We will continue to review our policies and procedures for ways to enhance the existing protections we have in place for our organization and continue to adapt to evolving threats.

As an additional resource, we are offering you a complimentary twelve (12) month membership of credit monitoring and identity theft protection services through IDX, A ZeroFox Company. This includes single bureau credit and CyberScan monitoring, fully managed ID theft recovery services, and access to a one-million-dollar (\$1,000,000) insurance reimbursement policy. With this protection, IDX will help you resolve issues if you suspect your identity is compromised. Instructions for how to enroll are below. Additional information about these services is also enclosed.

What You Can Do.

We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. We recommend you report errors or suspicious activity to your financial institution or the appropriate service provider. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation titled “Additional Steps to Help Protect Your Information” for contact information and resources you may take advantage of to protect against fraud or misuse, should you find it appropriate to do so.

You may enroll and take advantage of the offered IDX identity protection services by going to <https://app.idx.us/account-creation/protect> or calling 1-800-939-4170 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am – 8 pm Central Time. Please note the deadline to enroll is **November 1, 2024**.

For More Information.

Gamewell Mechanical is very sorry for any concern or inconvenience this incident has caused or may cause you, but please know that we remain committed to protecting the information entrusted in our care. If you have any other questions or concerns you may contact us at (804) 716-7712, during our standard business hours.

Sincerely,

Gamewell Mechanical, LLC
1417 Jake Alexander Blvd. S.
Salisbury, NC 28146



March 12, 2024



Para inscribirse, llame al:

1-800-939-4170

O visite:

<https://app.idx.us/account-creation/protect>

Código de inscripción:



Asunto: Aviso de incidente de privacidad de datos

Estimado/a [REDACTED]:

Gamewell Mechanical LLC se toma en serio la seguridad y la privacidad de los datos personales. Como parte de ese compromiso, le notificamos sobre un incidente reciente en el que podría haber visto involucrada su información personal. Lea esta carta detenidamente.

¿Qué sucedió?

Se notificó a Gamewell recientemente de actividad sospechosa de correo electrónico en la que vio involucrada una cuenta de correo electrónico de la empresa. De acuerdo con nuestros procedimientos, comenzamos de inmediato una investigación sobre la actividad que incluyó asociarnos con especialistas forenses informáticos para comprender la naturaleza y el alcance del incidente. El 19 de enero de 2024, confirmamos el acceso no autorizado a una cuenta de correo electrónico del empleado en varios momentos entre el 6 de diciembre de 2023 y el 17 de enero de 2024, por parte de alguien fuera de nuestra organización. Realizamos un análisis adicional de la cuenta afectada y determinamos que su información personal confidencial estaba dentro de la cuenta y posiblemente fue objeto de acceso no autorizado. Si bien no tenemos evidencia de que su información se haya filtrado o utilizado indebidamente, le notificamos por precaución.

¿Qué información se vio involucrada?

Usted recibe esta carta porque nuestra revisión confirmó que una persona desconocida tuvo acceso a su name, driver's license number, and date of birth. Enfatizamos que no tenemos indicios de que se haya filtrado información de la cuenta de correo electrónico o se haya utilizado indebidamente, pero le notificamos para que pueda aprovechar los recursos que le ofrecemos, en caso de que considere apropiado hacerlo.

Lo que estamos haciendo nosotros.

Además de asociarnos con especialistas forenses informáticos para investigar el incidente y comprender su naturaleza y alcance, continuamos requiriendo autenticación multifactor para las cuentas de correo electrónico de la empresa de todos los usuarios. Estamos notificando a las personas potencialmente afectadas por este incidente por precaución y le proporcionaremos recursos que puede aprovechar para proteger su información. Continuaremos revisando

nuestras políticas y procedimientos para encontrar formas de mejorar la protección que hemos implementado para nuestra organización y continuaremos adaptándonos a las amenazas en evolución.

Como recurso adicional, le ofrecemos una membresía gratuita de doce (12) meses de servicios de monitoreo de crédito y protección contra robo de identidad a través de IDX, una empresa de ZeroFox. Esto incluye el monitoreo de CyberScan y crédito de una sola oficina, servicios de recuperación de robo de identidad totalmente administrados y acceso a una póliza de reembolso de seguro de un millón de dólares (\$1,000,000). Con esta protección, IDX lo ayudará a resolver problemas si sospecha que su identidad se ha puesto en riesgo. A continuación, encontrará instrucciones sobre cómo inscribirse. También se adjunta información adicional sobre estos servicios.

Qué puede hacer usted.

Le recomendamos que esté atento a incidentes de fraude o uso indebido, desde cualquier fuente, revisando y monitoreando sus estados de cuenta e informes de crédito. Le recomendamos que informe de errores o actividades sospechosas a su institución financiera o al proveedor de servicios correspondiente. También puede presentar una denuncia ante las autoridades policíacas, el fiscal general de su estado y/o la Comisión Federal de Comercio. Consulte la documentación adjunta titulada “Pasos adicionales para ayudar a proteger su información” para obtener información de contacto y recursos que puede aprovechar para protegerse contra el fraude o el uso indebido, en caso de que considere apropiado hacerlo.

Puede inscribirse y aprovechar los servicios de protección de identidad de IDX ofrecidos visitando <https://app.idx.us/account-creation/protect> o llamando al 1-800-939-4170 y utilizando el Código de inscripción proporcionado anteriormente. Los representantes de IDX están disponibles de lunes a viernes de 8 a.m. a 8 p.m., hora del centro. Tenga en cuenta que la fecha límite para inscribirse es el **1.º de noviembre de 2024**.

Para obtener más información.

Gamewell Mechanical lamenta mucho cualquier inquietud o inconveniente que este incidente le haya causado o pueda causarle, pero debe saber que seguimos comprometidos a proteger la información que se confía a nuestro cuidado. Si tiene alguna otra pregunta o inquietud, puede comunicarse con nosotros al (804) 716-7712, en nuestro horario de atención estándar.

Atentamente,

Gamewell Mechanical, LLC
1417 Jake Alexander Blvd. S.
Salisbury, NC 28146

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax
1-888-298-0045
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com

Experian
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
1-800-680-7289
P.O. Box 2000
Chester, PA 19022
www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Initial fraud alerts will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for up to seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online using the above contact information. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online using the above contact information. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

Obtain Additional Information about the steps you can take to avoid identity theft from the following entities:

- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division may be contacted at 200 St. Paul Place, 16th Flr., Baltimore, MD 21202, www.marylandattorneygeneral.gov, and toll-free at (888) 743-0023 or (410) 528-8662;

- **North Carolina Residents:** Office of the Attorney General of North Carolina may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, <https://ncdoj.gov>, (919) 716-6400; and
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338). This notification was not delayed by law enforcement.



- | |
|--|
| <p>1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.</p> |
| <p>2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.</p> |
| <p>3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.</p> |
| <p>4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring.</p> |

SINGLE BUREAU CREDIT MONITORING (adults) - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

PASOS ADICIONALES PARA AYUDAR A PROTEGER SU INFORMACIÓN

Revise los estados de cuenta personales y los informes de crédito. Le recomendamos que siga atento revisando los estados de cuenta personales y monitoreando los informes de crédito para detectar cualquier error o actividad no autorizada. En virtud de la ley federal, usted también tiene derecho cada 12 meses a una copia gratuita de su informe de crédito de cada una de las tres principales empresas de informes de crédito. Para obtener un informe de crédito anual gratuito, visite www.annualcreditreport.com o llame al (877) 322-8228. Es posible que desee escalar sus solicitudes para recibir un informe gratuito de una de las tres agencias de informes de crédito cada cuatro meses. Si descubre algún elemento sospechoso, debe informar de cualquier información incorrecta en su informe a la agencia de informes de crédito. Los nombres y la información de contacto de las agencias de informes de crédito son:

Equifax
1-888-298-0045
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com

Experian
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
1-800-680-7289
P.O. Box 2000
Chester, PA 19022
www.transunion.com

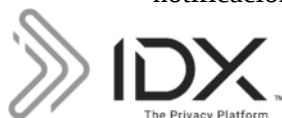
Reporte sospechas de fraude. Tiene derecho a presentar una denuncia policiaca si alguna vez es víctima de un fraude de identidad. Tenga en cuenta que para presentar un informe de delito o un informe de incidente ante las autoridades por robo de identidad, es probable que deba proporcionar algún tipo de prueba de que ha sido víctima. A menudo se requiere una denuncia policiaca para disputar artículos fraudulentos. Debe informar de los presuntos incidentes de robo de identidad a las autoridades locales, al fiscal general de su estado y/o a la Comisión Federal de Comercio.

Establecer alertas de fraude. Una alerta de fraude les indica a las empresas que verifican su crédito que deben consultar con usted antes de abrir una cuenta nueva. Las alertas de fraude iniciales durarán un año. Las alertas de fraude son gratuitas y las víctimas de robo de identidad pueden recibir una alerta de fraude extendida por hasta siete años. Si elige establecer una alerta de fraude, le recomendamos que haga esto después de activar su monitoreo de crédito. Para establecer una alerta de fraude, comuníquese con las agencias nacionales de informes de crédito por teléfono o en línea utilizando la información de contacto anterior. Para obtener más información, visite <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Establezca un congelamiento de seguridad. Los congelamientos de seguridad, también conocidos como congelamientos de crédito, restringen el acceso a su expediente de crédito, lo que dificulta que los ladrones de identidad abran nuevas cuentas en su nombre. Puede congelar y descongelar su expediente de crédito de forma gratuita. También puede obtener un congelamiento gratuito para sus hijos menores de 16 años. Y si usted es el tutor, custodio o tiene un poder notarial válido, también puede obtener un congelamiento gratuito para esa persona. Para implementar un congelamiento de seguridad, comuníquese con las agencias nacionales de informes de crédito por teléfono o en línea utilizando la información de contacto anterior. Si solicita un congelamiento en línea o por teléfono, la agencia debe establecer el congelamiento dentro de un día hábil. Si solicita un descongelamiento, la agencia debe descongelarlo en el plazo de una hora. Si realiza su solicitud por correo, la agencia debe establecer o levantar un congelamiento dentro de los tres días hábiles después de recibir su solicitud. También puede descongelarlo temporalmente sin cargo. Además, no confunda los congelamientos con los bloqueos. Funcionan de manera similar, pero los bloqueos pueden tener cargos mensuales. Si desea un congelamiento gratuito garantizado por la ley federal, opte por un congelamiento, no un bloqueo. Para obtener más información, visite <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

Obtenga información adicional de las medidas que puede tomar para evitar el robo de identidad de las siguientes entidades:

- **Residentes de Maryland:** puede comunicarse con la Oficina del Fiscal General de Maryland, División de Protección al Consumidor, en 200 St. Paul Place, 16th Flr., Baltimore, MD 21202, www.marylandattorneygeneral.gov, y al número gratuito (888) 743-0023 o (410) 528-8662.
- **Residentes de Carolina del Norte:** puede comunicarse con la Oficina del Fiscal General de Carolina del Norte en 9001 Mail Service Center, Raleigh, NC 27699-9001, <https://ncdoj.gov>, (919) 716-6400.
- **Todos los residentes de EE. UU.:** puede comunicarse con Identity Theft Clearinghouse, Federal Trade Commission en 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338). Esta notificación no fue retrasada por las fuerzas policíacas.



1. Sitio web e inscripción. Visite <https://app.idx.us/account-creation/protect> y siga las instrucciones para la inscripción utilizando el código de inscripción que se le proporciona en la parte superior de la carta.

2. Active el monitoreo de crédito proporcionado como parte de su membresía de protección de identidad de IDX. El monitoreo incluido en la membresía debe activarse para que entre en vigencia. Nota: Debe haber establecido crédito y tener acceso a una computadora e Internet para usar este servicio. Si necesita ayuda, IDX podrá ayudarle.

3. Revise sus informes de crédito. Le recomendamos que siga atento revisando los estados de cuenta y monitoreando los informes de crédito. Si descubre algún elemento sospechoso y se ha inscrito en la protección de identidad de IDX, notifíquelo de inmediato llamando o iniciando sesión en el sitio web de IDX y presentando una solicitud de ayuda. Si presenta una solicitud de ayuda o informa de una actividad sospechosa, un miembro de nuestro equipo de ID Care se comunicará con usted para ayudarle a determinar la causa de los elementos sospechosos. En el improbable caso de que sea víctima de robo de identidad como consecuencia de este incidente, se le asignará un especialista en cuidado de identidad que trabajará en su nombre para identificar, detener y revertir el daño rápidamente.

4. Establezca alertas de fraude con las tres agencias de informes de crédito. Si elige establecer una alerta de fraude, le recomendamos que haga esto después de activar su monitoreo de crédito.

MONITOREO DE CRÉDITO DE BUREAU ÚNICO (adultos): monitoreo de la oficina de crédito para detectar cambios en el archivo de crédito del miembro, como nuevas consultas de crédito, nuevas cuentas abiertas, pagos retrasados, mejoras en el informe de crédito del miembro, quiebras, sentencias judiciales y gravámenes fiscales, nuevas direcciones, nuevos empleadores y otras actividades que afecten el registro de crédito del miembro.

CYBERSCAN™: monitoreo en la web oscura de sitios web clandestinos, salas de chat y malware, las 24 horas del día, los siete días de la semana, para identificar el comercio o la venta de información personal como números de Seguro Social, cuentas bancarias, direcciones de correo electrónico, números de identificación médica, números de licencia de conducir, números de pasaporte, tarjetas de crédito y débito, números de teléfono y otros identificadores únicos.

SEGURO CONTRA ROBO DE IDENTIDAD: el seguro contra robo de identidad reembolsará a los miembros los gastos asociados con la restauración de su identidad en caso de que sean víctimas de robo de identidad. Si la identidad de un miembro se ve comprometida, la póliza proporciona cobertura de hasta \$1,000,000, sin deducible, de una aseguradora “con calificación A” por A.M. Best. La cobertura está sujeta a los términos, límites y/o exclusiones de la póliza.

RECUPERACIÓN DE IDENTIDAD COMPLETAMENTE ADMINISTRADA: el servicio de recuperación completamente administrado de IDX proporciona restauración para problemas de robo de identidad, como (entre otros) apertura de cuentas, robo de identidad criminal, robo de identidad médica, adquisición de cuentas, solicitud de alquiler, fraude fiscal, fraude de prestaciones y contratación de servicios públicos. Este servicio incluye un proceso de clasificación completo para las personas afectadas que informan de actividades sospechosas, un especialista de IDCare asignado personalmente para gestionar completamente la restauración de cada caso y orientación experta para personas con preguntas sobre robo de identidad y medidas de protección.