

EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Turner Construction Company (“Turner”) does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

Turner recently identified a cybersecurity incident involving unauthorized access to certain Turner systems. Upon discovering the activity, Turner took steps to secure its systems, engaged leading third-party cybersecurity experts, and began an investigation.

The investigation determined that there was unauthorized access to certain Turner systems between July 2 and July 15, 2026. On July 27, 2026, Turner confirmed that files containing personal information had been accessed without authorization.

The files identified during the review contained one or more of the following categories of personal information: name, Social Security number (for individuals in the United States), Social Insurance Number (for individuals in Canada), date of birth, salary, bank account information used for direct deposit, and home address. For a limited number of individuals, the files may also have contained a passport number.

Notice to Washington Residents

On or about August 18, 2026, Turner provided written notice of this incident to approximately three thousand four hundred one (3,401) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Turner moved quickly to investigate and respond to the incident, assess the security of Turner systems, and identify potentially affected individuals. Further, Turner notified federal law enforcement regarding the event. Turner is also working to implement additional safeguards and training to its employees. Turner is providing access to credit monitoring services for five (5) years, through IDX and IDShield, to individuals whose personal information was potentially involved in this incident, at no cost to these individuals.

Additionally, Turner is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Turner is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Turner is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A



P.O. Box 1907
Suwanee, GA 30024

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

August 18, 2026

<<NOTICE OF DATA BREACH>>

Dear <<Name 1>> <<Name 2>>:

Turner Construction Company is writing to notify you of a cybersecurity incident involving your personal information. We are providing information about the incident, our response, the services available to you, and steps you can take to help protect against identity theft and fraud.

What Happened?

Turner recently identified a cybersecurity incident involving unauthorized access to certain Turner systems. Upon discovering the activity, Turner took steps to secure its systems, engaged leading third-party cybersecurity experts, and began an investigation.

The investigation determined that there was unauthorized access to certain Turner systems between July 2 and July 15, 2026. On July 27, 2026, Turner confirmed that files containing personal information had been accessed without authorization.

During a detailed review of the affected files, conducted with the assistance of leading third-party cybersecurity experts, Turner identified files contained personal information relating to you. As a result, we are notifying you of this incident and providing information about the resources available to help protect your personal information.

What Information Was Involved?

The files identified during the review contained one or more of the following categories of personal information: name, Social Security number (for individuals in the United States), Social Insurance Number (for individuals in Canada), date of birth, salary, bank account information used for direct deposit, and home address. For a limited number of individuals, the files may also have contained a passport number.

Our Response.

We understand this news may cause concern for you. We regret the concern and inconvenience this incident may cause and are committed to supporting you with information, resources, and identity protection services. The confidentiality, privacy, and security of information within our care are among Turner's highest priorities. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our information-security practices, strengthening existing safeguards, and implementing additional measures based on the findings of our investigation and recommendations from cybersecurity experts.

What You Can Do.

Turner is offering you identity monitoring, identity restoration, and related support services from IDShield at no cost to you for five years. You must enroll to access this benefit. Enrollment instructions and information on their services are enclosed.

The IDShield protection plan provides the following:

- Monitors personal identifiable information such as social security numbers, passport numbers, driver's licenses, bank accounts, login credentials, User ID's and immediately alerts you if any risk is detected.
- Assigns a licensed private investigator to restore your identity to pre-theft status in the case of identity theft—including pre-existing events.
- Assigns identity theft specialists available for consultation and advice about identity theft or online privacy concerns.
- Provides 24/7/365 emergency support, as well as a mobile app, which you can use to check your monthly credit score, review identity threat alerts, and obtain emergency assistance

In addition to enrolling in identity monitoring services, we encourage you to remain vigilant by:

- Reviewing your bank, credit card, retirement, and other financial accounts for activity you do not recognize.
- Enabling account alerts and multi-factor authentication where available.
- Reviewing your credit reports for unfamiliar accounts or inquiries.
- Considering a fraud alert or credit freeze.
- Being cautious of unexpected emails, text messages, or telephone calls requesting personal or financial information.
- Contacting your financial institution and IDShield immediately if you notice suspicious activity.

Additional guidance is included in the enclosed **Steps You Can Take to Protect Your Personal Information**.

For questions about enrollment or the identity protection services, contact IDShield at 888-807-0407 and membersupport@legalshieldcorp.com.

If you have questions about the incident or need assistance, please contact the Turner Identity Protection Response Team at **1-866-688-9340** or **TurnerIdentityProtection@tcco.com**. You can also contact our call center at 1-866-200-0984 Monday – Friday, 9 am – 9 pm ET with questions.

You may also write to:

Turner Construction Company
66 Hudson Boulevard East
New York, NY 10001

Sincerely,

Aaron Wiebelhaus
Chief People Officer
Turner Construction Company

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Activate your IDShield Account

1. Enroll at: access.legalshield.com.
2. You will be asked to enter your date of birth and social security number; this is safe to do so.
3. Verify your identity. Select IDShield from your Member Portal and click “Start” to answer the verification questions
4. Add your information to monitor.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should you wish to place a fraud alert, please contact one of the three major credit reporting bureaus listed below. If you wish to place a credit freeze, you must contact each of the three major credit reporting agencies.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://oag.maryland.gov>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<#>> Rhode Island residents that may be impacted by this event.



P.O. Box 1907
Suwanee, GA 30024

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

18 de agosto de 2026

<<AVISO DE FILTRACIÓN DE DATOS>>

Estimado/a <<Name 1>> <<Name 2>>:

Turner Construction Company le escribe para informarle de un incidente reciente de ciberseguridad que involucra su información personal. Le proporcionamos información sobre el incidente, nuestra respuesta, los servicios que tiene a su disposición y las medidas que puede tomar para protegerse contra el robo de identidad y el fraude.

¿Qué sucedió?

Turner ha detectado recientemente un incidente de ciberseguridad relacionado con el acceso no autorizado a determinados sistemas de Turner. Al descubrir la actividad, Turner tomó medidas para proteger sus sistemas, contrató a expertos externos líderes en ciberseguridad y puso en marcha una investigación.

La investigación determinó que hubo un acceso no autorizado a determinados sistemas de Turner entre el 2 de julio y el 15 de julio de 2026. El 27 de julio de 2026, Turner confirmó que se había accedido a expedientes que contenían información personal.

Durante un análisis detallado de los expedientes afectados, que se realizó con la ayuda de expertos externos de primer nivel en ciberseguridad, Turner identificó expedientes que contenían información personal relacionada con usted. Por ello, le informamos de este incidente y le facilitamos información sobre los recursos disponibles para ayudarlo a proteger sus datos personales.

¿Qué información se vio involucrada?

Los expedientes identificados durante la revisión contenían una o varias de las siguientes categorías de datos personales: nombre, número del Seguro Social (SS) para personas residentes en Estados Unidos, número de Seguro social (SIN), para personas residentes en Canadá, fecha de nacimiento, salario, datos de cuentas bancarias utilizadas para el ingreso directo y dirección particular. En el caso de un número limitado de personas, es posible que los expedientes también incluyeran el número de pasaporte.

Nuestra respuesta.

Comprendemos que esta noticia pueda preocuparle. Lamentamos la preocupación y las molestias que este incidente pueda ocasionar, y nos comprometemos a ofrecerle apoyo mediante información, recursos y servicios de protección de identidad. La confidencialidad, la privacidad y la seguridad de la información a nuestro cuidado figuran entre las principales prioridades de Turner. Como parte de nuestro compromiso constante con la privacidad de la información que tenemos a nuestro cargo, estamos revisando nuestras prácticas de seguridad de la información, reforzando las medidas de protección

existentes y aplicando medidas adicionales basadas en las conclusiones de nuestra investigación y en las recomendaciones de los expertos en ciberseguridad.

Qué puede hacer.

Turner le ofrece servicios de monitoreo de identidad, recuperación de identidad y otros servicios de asistencia relacionados de IDShield, sin costo para usted durante cinco años. Debe inscribirse para acceder a este beneficio. Se adjuntan las instrucciones para inscribirse e información sobre estos servicios.

El plan de protección IDShield ofrece lo siguiente:

- Monitoreo de información de identificación personal, como números de Seguro Social, números de pasaporte, licencias de conducir, cuentas bancarias, credenciales de inicio de sesión e identificaciones de usuario, y le avisa de inmediato si se detecta algún riesgo.
- En caso de robo de identidad, le asigna un investigador privado con licencia para ayudarlo a recuperar su identidad a la situación anterior al robo, incluso si se tratara de incidentes ocurridos previamente.
- Asigna especialistas en robo de identidad que están disponibles para brindarle orientación y asesoramiento sobre el robo de identidad o inquietudes relacionadas con la privacidad en línea.
- Brinda asistencia de emergencia las 24 horas del día, los 7 días de la semana, los 365 días del año, además de una aplicación móvil que puede usar para consultar su calificación crediticia mensual, revisar las alertas sobre amenazas a su identidad y obtener asistencia de emergencia

Además de contratar servicios de monitoreo de identidad, le recomendamos que se mantenga alerta de la siguiente manera:

- Revise sus cuentas bancarias, de tarjetas de crédito, de jubilación y demás cuentas financieras para detectar cualquier movimiento que no reconozca.
- Active las alertas de las cuentas y la autenticación multifactorial cuando estén disponibles.
- Revise sus informes de crédito para detectar cuentas o consultas que no le resulten conocidas.
- Considere la activación de una alerta de fraude o un congelamiento de crédito.
- Desconfíe de correos electrónicos, mensajes de texto o llamadas telefónicas inusuales en los que se solicite información personal o financiera.
- Comuníquese con su entidad financiera y con IDShield de inmediato si detecta alguna actividad sospechosa.

Se incluye orientación adicional en el documento adjunto, **Medidas que puede tomar para proteger la información personal**.

Si tiene preguntas sobre la inscripción o los servicios de protección de identidad, comuníquese con IDShield llamando al 888-807-0407 o escribiendo a membersupport@legalshieldcorp.com.

Si tiene alguna pregunta sobre el incidente o necesita ayuda, comuníquese con el Equipo de Respuesta para la Protección de Identidad de Turner llamando al **1-866-688-9340** o escribiendo a **TurnerIdentityProtection@tcco.com**. También puede comunicarse con nuestro centro de atención telefónica al 1-866-200-0984, de lunes a viernes de 9 a. m. a 9 p. m., hora del Este, si tiene preguntas.

También puede escribir a:

Turner Construction Company
66 Hudson Boulevard East
New York, NY 10001

Atentamente,

Aaron Wiebelhaus
Director de Recursos Humanos
Turner Construction Company

MEDIDAS QUE PUEDE TOMAR PARA PROTEGER LA INFORMACIÓN PERSONAL

Activar su cuenta de IDShield

1. Inscribese en: access.legalshield.com.
2. Se le pedirá que ingrese su fecha de nacimiento y su número de seguro social. Puede hacerlo, es seguro.
3. Verifique su identidad. Seleccione IDShield en su Portal para Miembros y haga clic en “Comenzar” para responder las preguntas de verificación
4. Añada su información para monitoreo.

Monitoree sus cuentas

Según la ley de los EE. UU., el consumidor tiene derecho a solicitar un informe de crédito gratuito por año de cada una de las tres principales agencias de informes de crédito: Equifax, Experian y TransUnion. Para solicitar un informe de crédito gratuito, visite www.annualcreditreport.com o llame al número gratuito 1-877-322-8228. Los consumidores también pueden comunicarse directamente con las tres principales agencias de informes de crédito que se enumeran a continuación para solicitar una copia gratuita de su informe crediticio.

Los consumidores tienen derecho a colocar una “alerta de fraude” inicial o extendida en un expediente de crédito, sin costo alguno. Una alerta de fraude inicial es una alerta que dura un año y que se incluye en el expediente de crédito del consumidor. Al ver una alerta de fraude en el expediente de crédito de un consumidor, una empresa está obligada a tomar medidas para verificar la identidad del consumidor antes de concederle un nuevo crédito. Si los consumidores son víctimas de robo de identidad, tienen derecho a una alerta de fraude extendida, que es una alerta de fraude de siete años de duración. Si los consumidores desean colocar una alerta de fraude, deben comunicarse con cualquiera de las tres principales agencias de informes de crédito que se enumeran a continuación.

Como alternativa a una alerta de fraude, los consumidores tienen derecho a colocar un “congelamiento de crédito” en un informe de crédito, lo que prohibirá que una agencia de crédito divulgue información en el informe de crédito sin la autorización expresa del consumidor. El congelamiento de crédito está diseñado para evitar que el crédito, los préstamos y los servicios se aprueben en nombre de un consumidor sin su consentimiento. Sin embargo, los consumidores deben saber que el uso de un congelamiento de crédito para controlar quién tiene acceso a la información personal y financiera en su informe crediticio puede retrasar, interferir o prohibir la aprobación oportuna de cualquier pedido o solicitud posterior que realicen con respecto a un nuevo préstamo, crédito, hipoteca, o cualquier otra cuenta que implique la concesión de un crédito. De conformidad con la ley federal, no se puede cobrar a los consumidores por colocar o levantar un congelamiento de crédito en su informe crediticio. Para solicitar un congelamiento de crédito, es posible que las personas deban proporcionar parte o la totalidad de la siguiente información:

1. Nombre completo (incluida la inicial del segundo nombre, así como Jr., Sr., III, etc.);
2. Número de Seguro Social;
3. Fecha de nacimiento;
4. Domicilios en los últimos dos a cinco años;
5. Comprobante de domicilio, como una factura actual de servicios públicos o de teléfono;
6. Fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir estatal o tarjeta de identificación estatal, etc.); y
7. Copia de la denuncia policial el informe de la investigación o la reclamación ante una agencia de orden público respecto del robo de identidad si es víctima de este delito.

Si desea colocar una alerta de fraude, comuníquese con una de las tres principales agencias de informes de crédito que se enumeran a continuación. Para colocar un congelamiento de crédito, debe comunicarse con cada una de las tres agencias de informes de crédito principales.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Información adicional

Los consumidores pueden informarse aún más sobre el robo de identidad, las alertas de fraude, las congelaciones de crédito y las medidas que pueden tomar para proteger su información personal poniéndose en contacto con las agencias de informes del consumidor, la Comisión Federal de Comercio o el Fiscal General de su estado. Puede comunicarse con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261. La Comisión Federal de Comercio también recomienda a quienes descubran un uso indebido de su información que presenten una reclamación ante ella. Los consumidores pueden obtener más información sobre cómo presentar dicha reclamación a través de la información de contacto mencionada anteriormente. Los consumidores tienen derecho a presentar una denuncia policial si alguna vez sufren un robo de identidad o un fraude. Tenga en cuenta que, para presentar una denuncia ante las autoridades policiales por robo de identidad, es probable que los consumidores deban proporcionar alguna prueba de que han sido víctimas. Los casos de robo de identidad conocido o presuntos también deben informarse a las autoridades policiales y al Fiscal General del estado correspondiente. Las autoridades policiales no han aplazado este aviso.

Los residentes del Distrito de Columbia pueden comunicarse con el fiscal general del Distrito de Columbia en: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; y oag.dc.gov.

Los residentes de Maryland pueden comunicarse con el fiscal general de Maryland en: 200 St. Paul Place, 16th Floor, Baltimore, MD, al 21202; 1-410-576-6300 o al 1-888-743-0023 y en <https://oag.maryland.gov>.

Para los residentes de Nuevo México, los consumidores tienen derechos de conformidad con la Ley de Informes de Crédito Justos, como el derecho a que se les informe si los datos de su expediente de crédito se ha utilizado en su contra, el derecho a saber qué figura en su expediente de crédito, el derecho a solicitar su calificación crediticia y el derecho a objetar información incompleta o inexacta. Además, de conformidad con la Ley de Informes de Crédito Justos, las agencias de informes de los consumidores deben corregir o eliminar información inexacta, incompleta o no verificable; las agencias de informes de los consumidores no pueden reportar información negativa obsoleta; el acceso a los expedientes de los consumidores es limitado; los consumidores deben dar su consentimiento para que se proporcionen informes de crédito a los empleadores; los consumidores pueden limitar las ofertas de crédito y de seguro "preseleccionadas" basadas en la información de su informe de crédito; y los consumidores pueden solicitar daños y perjuicios a los infractores. Los consumidores pueden tener derechos adicionales conforme a la Ley de Informes de Crédito Justos, que no figuran aquí. Las víctimas del robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos conforme a la Ley de Informes de Crédito Justos. Le recomendamos que consulte sus derechos conforme a la Ley de Informes de Crédito Justos visitando www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o escribiendo a Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Los residentes de Nueva York pueden comunicarse con el fiscal general de Nueva York en Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

Los residentes de Carolina del Norte pueden comunicarse con el fiscal general de Carolina del Norte en: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 o 1-919-716-6000; y www.ncdoj.gov.

Los residentes de Rhode Island pueden comunicarse con el fiscal general de Rhode Island en: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Según la ley de Rhode Island, las personas tienen derecho a obtener cualquier informe policial presentado con respecto a este evento. Existen aproximadamente <<#>> residentes de Rhode Island que pueden verse afectados por este evento.



P.O. Box 1907
Suwanee, GA 30024

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: November 18, 2026

To Enroll, Scan the QR Code Below:



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

August 18, 2026

<<NOTICE OF DATA BREACH>>

Dear <<Name 1>> <<Name 2>>:

Turner Construction Company is writing to notify you of a cybersecurity incident involving your personal information. We are providing information about the incident, our response, the services available to you, and steps you can take to help protect against identity theft and fraud.

What Happened?

Turner recently identified a cybersecurity incident involving unauthorized access to certain Turner systems. Upon discovering the activity, Turner took steps to secure its systems, engaged leading third-party cybersecurity experts, and began an investigation.

The investigation determined that there was unauthorized access to certain Turner systems between July 2 and July 15, 2026. On July 27, 2026, Turner confirmed that files containing personal information had been accessed without authorization.

During a detailed review of the affected files, conducted with the assistance of leading third-party cybersecurity experts, Turner identified files contained personal information relating to you. As a result, we are notifying you of this incident and providing information about the resources available to help protect your personal information.

What Information Was Involved?

The files identified during the review contained one or more of the following categories of personal information: name, Social Security number (for individuals in the United States), Social Insurance Number (for individuals in Canada), date of birth, salary, bank account information used for direct deposit, and home address. For a limited number of individuals, the files may also have contained a passport number.

Our Response.

We understand this news may cause concern for you. We regret the concern and inconvenience this incident may cause and are committed to supporting you with information, resources, and identity protection services. The confidentiality, privacy, and security of information within our care are among Turner's highest priorities. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our information-security practices, strengthening existing safeguards, and implementing additional measures based on the findings of our investigation and recommendations from cybersecurity experts.

What You Can Do.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: five years of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. You must enroll to access this benefit.

In addition to enrolling in identity monitoring services, we encourage you to remain vigilant by:

- Reviewing your bank, credit card, retirement, and other financial accounts for activity you do not recognize.
- Enabling account alerts and multi-factor authentication where available.
- Reviewing your credit reports for unfamiliar accounts or inquiries.
- Considering a fraud alert or credit freeze.
- Being cautious of unexpected emails, text messages, or telephone calls requesting personal or financial information.
- Contacting your financial institution and IDX immediately if you notice suspicious activity.

Additional guidance is included in the enclosed **Steps You Can Take to Protect Your Personal Information**.

For questions about enrollment or the identity protection services, contact 1-866-200-0984 Monday – Friday, 9 am – 9 pm ET.

If you have questions about the incident or need assistance, please contact the Turner Identity Protection Response Team at **1-866-688-9340** or **TurnerIdentityProtection@tcco.com**.

You may also write to:

Turner Construction Company
66 Hudson Boulevard East
New York, NY 10001

Sincerely,

Aaron Wiebelhaus
Chief People Officer
Turner Construction Company

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

1. Website and Enrollment. Scan the QR image or 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. Please note the deadline to enroll is November 18, 2026.

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.

3. Telephone. Contact IDX at 1-866-200-0984 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should you wish to place a fraud alert, please contact one of the three major credit reporting bureaus listed below. If you wish to place a credit freeze, you must contact each of the three major credit reporting agencies.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://oag.maryland.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<#>> Rhode Island residents that may be impacted by this event.



P.O. Box 1907
Suwanee, GA 30024

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Código de inscripción: <<XXXXXXXXXX>>

Fecha límite de inscripción: 18 de
noviembre de 2026

Para inscribirse, escanee el código QR a
continuación:



O visite:

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

18 de agosto de 2026

<<AVISO DE FILTRACIÓN DE DATOS>>

Estimado/a <<Name 1>> <<Name 2>>:

Turner Construction Company le escribe para informarle de un incidente reciente de ciberseguridad que involucra su información personal. Le proporcionamos información sobre el incidente, nuestra respuesta, los servicios que tiene a su disposición y las medidas que puede tomar para protegerse contra el robo de identidad y el fraude.

¿Qué sucedió?

Turner ha detectado recientemente un incidente de ciberseguridad relacionado con el acceso no autorizado a determinados sistemas de Turner. Al descubrir la actividad, Turner tomó medidas para proteger sus sistemas, contrató a expertos externos líderes en ciberseguridad y puso en marcha una investigación.

La investigación determinó que hubo un acceso no autorizado a determinados sistemas de Turner entre el 2 de julio y el 15 de julio de 2026. El 27 de julio de 2026, Turner confirmó que se había accedido a expedientes que contenían información personal.

Durante un análisis detallado de los expedientes afectados, que se realizó con la ayuda de expertos externos de primer nivel en ciberseguridad, Turner identificó expedientes que contenían información personal relacionada con usted. Por ello, le informamos de este incidente y le facilitamos información sobre los recursos disponibles para ayudarle a proteger sus datos personales.

¿Qué información se vio involucrada?

Los expedientes identificados durante la revisión contenían una o varias de las siguientes categorías de datos personales: nombre, número del Seguro Social (SS) para personas residentes en Estados Unidos, número de Seguro social (SIN), para personas residentes en Canadá, fecha de nacimiento, salario, datos de cuentas bancarias utilizadas para el ingreso directo y dirección particular. En el caso de un número limitado de personas, es posible que los expedientes también incluyeran el número de pasaporte.

Nuestra respuesta.

Comprendemos que esta noticia pueda preocuparle. Lamentamos la preocupación y las molestias que este incidente pueda ocasionar, y nos comprometemos a ofrecerle apoyo mediante información, recursos y servicios de protección de identidad. La confidencialidad, la privacidad y la seguridad de la información a nuestro cuidado figuran entre las principales prioridades de Turner. Como parte de nuestro compromiso constante con la privacidad de la información que tenemos a nuestro cargo, estamos revisando nuestras prácticas de seguridad de la información, reforzando las medidas de protección existentes y aplicando medidas adicionales basadas en las conclusiones de nuestra investigación y en las recomendaciones de los expertos en ciberseguridad.

Qué puede hacer.

Además, ofrecemos servicios de protección contra el robo de identidad a través de IDX, experta en servicios de filtración y recuperación de datos. Los servicios de protección de identidad de IDX incluyen: cinco años de monitoreo de crédito y CyberScan, una póliza de seguro de reembolso de \$1,000,000 y la administración total de los servicios de recuperación de robo de identidad. Debe inscribirse para acceder a este beneficio.

Además de contratar servicios de monitoreo de identidad, le recomendamos que se mantenga alerta de la siguiente manera:

- Revise sus cuentas bancarias, de tarjetas de crédito, de jubilación y demás cuentas financieras para detectar cualquier movimiento que no reconozca.
- Active las alertas de las cuentas y la autenticación multifactorial cuando estén disponibles.
- Revise sus informes de crédito para detectar cuentas o consultas que no le resulten conocidas.
- Considere la activación de una alerta de fraude o un congelamiento de crédito.
- Desconfíe de correos electrónicos, mensajes de texto o llamadas telefónicas inusuales en los que se solicite información personal o financiera.
- Comuníquese con su entidad financiera y con IDX de inmediato si detecta alguna actividad sospechosa.

Se incluye orientación adicional en el documento adjunto, **Medidas que puede tomar para proteger la información personal**.

Si tiene preguntas sobre la inscripción o los servicios de protección de identidad, llame al 1-866-200-0984, de lunes a viernes de 9 a. m. a 9 p. m., hora del Este.

Si tiene alguna pregunta sobre el incidente o necesita ayuda, comuníquese con el Equipo de Respuesta para la Protección de Identidad de Turner llamando al **1-866-688-9340** o escribiendo a **TurnerIdentityProtection@tcco.com**.

También puede escribir a:

Turner Construction Company
66 Hudson Boulevard East
New York, NY 10001

Atentamente,

Aaron Wiebelhaus
Director de Recursos Humanos
Turner Construction Company

Medidas que puede tomar para proteger la información personal

1. Sitio web e inscripción. Escanee la imagen QR o visite <https://app.idx.us/account-creation/protect> y siga las instrucciones de inscripción utilizando el código de inscripción que se le proporciona en la parte superior de la carta. Tenga en cuenta que la fecha límite para inscribirse es el 18 de noviembre de 2026.

2. Active el monitoreo de crédito proporcionado como parte de su membresía en la protección de identidad de IDX. El monitoreo incluido en la membresía debe estar activado para que sea operativo. Nota: Para poder utilizar este servicio debe tener un crédito establecido, y acceso a una computadora y a internet. Si necesita asistencia, IDX podrá ayudarlo.

3. Teléfono. Comuníquese con IDX al 1-866-200-0984 para obtener más información sobre este evento y hablar con representantes expertos sobre las medidas apropiadas que debe tomar para proteger su identidad crediticia.

Monitoree sus cuentas

Según la ley de los EE. UU., el consumidor tiene derecho a solicitar un informe de crédito gratuito por año de cada una de las tres principales agencias de informes de crédito: Equifax, Experian y TransUnion. Para solicitar un informe de crédito gratuito, visite www.annualcreditreport.com o llame al número gratuito 1-877-322-8228. Los consumidores también pueden comunicarse directamente con las tres principales agencias de informes de crédito que se enumeran a continuación para solicitar una copia gratuita de su informe crediticio.

Los consumidores tienen derecho a colocar una “alerta de fraude” inicial o extendida en un expediente de crédito, sin costo alguno. Una alerta de fraude inicial es una alerta que dura un año y que se incluye en el expediente de crédito del consumidor. Al ver una alerta de fraude en el expediente de crédito de un consumidor, una empresa está obligada a tomar medidas para verificar la identidad del consumidor antes de concederle un nuevo crédito. Si los consumidores son víctimas de robo de identidad, tienen derecho a una alerta de fraude extendida, que es una alerta de fraude de siete años de duración. Si los consumidores desean colocar una alerta de fraude, deben comunicarse con cualquiera de las tres principales agencias de informes de crédito que se enumeran a continuación.

Como alternativa a una alerta de fraude, los consumidores tienen derecho a colocar un “congelamiento de crédito” en un informe de crédito, lo que prohibirá que una agencia de crédito divulgue información en el informe de crédito sin la autorización expresa del consumidor. El congelamiento de crédito está diseñado para evitar que el crédito, los préstamos y los servicios se aprueben en nombre de un consumidor sin su consentimiento. Sin embargo, los consumidores deben saber que el uso de un congelamiento de crédito para controlar quién tiene acceso a la información personal y financiera en su informe crediticio puede retrasar, interferir o prohibir la aprobación oportuna de cualquier pedido o solicitud posterior que realicen con respecto a un nuevo préstamo, crédito, hipoteca, o cualquier otra cuenta que implique la concesión de un crédito. De conformidad con la ley federal, no se puede cobrar a los consumidores por colocar o levantar un congelamiento de crédito en su informe crediticio. Para solicitar un congelamiento de crédito, es posible que las personas deban proporcionar parte o la totalidad de la siguiente información:

1. Nombre completo (incluida la inicial del segundo nombre, así como Jr., Sr., III, etc.);
2. Número de Seguro Social;
3. Fecha de nacimiento;
4. Domicilios en los últimos dos a cinco años;
5. Comprobante de domicilio, como una factura actual de servicios públicos o de teléfono;
6. Fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir estatal o tarjeta de identificación estatal, etc.); y
7. Copia de la denuncia policial el informe de la investigación o la reclamación ante una agencia de orden público respecto del robo de identidad si es víctima de este delito.

Si desea colocar una alerta de fraude, comuníquese con una de las tres principales agencias de informes de crédito que se enumeran a continuación. Para colocar un congelamiento de crédito, debe comunicarse con cada una de las tres agencias de informes de crédito principales.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Información adicional

Los consumidores pueden informarse aún más sobre el robo de identidad, las alertas de fraude, las congelaciones de crédito y las medidas que pueden tomar para proteger su información personal poniéndose en contacto con las agencias de informes del consumidor, la Comisión Federal de Comercio o el Fiscal General de su estado. Puede comunicarse con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261. La Comisión Federal de Comercio también recomienda a quienes descubran un uso indebido de su información que presenten una reclamación ante ella. Los consumidores pueden obtener más información sobre cómo presentar dicha reclamación a través de la información de contacto mencionada anteriormente. Los consumidores tienen derecho a presentar una denuncia policial si alguna vez sufren un robo de identidad o un fraude. Tenga en cuenta que, para presentar una denuncia ante las autoridades policiales por robo de identidad, es probable que los consumidores deban proporcionar alguna prueba de que han sido víctimas. Los casos de robo de identidad conocido o presuntos también deben informarse a las autoridades policiales y al Fiscal General del estado correspondiente. Las autoridades policiales no han aplazado este aviso.

Los residentes del Distrito de Columbia pueden comunicarse con el fiscal general del Distrito de Columbia en: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; y oag.dc.gov.

Los residentes de Maryland pueden comunicarse con el fiscal general de Maryland en: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 o 1-888-743-0023; y <https://oag.maryland.gov>.

Para los residentes de Nuevo México, los consumidores tienen derechos de conformidad con la Ley de Informes de Crédito Justos, como el derecho a que se les informe si los datos de su expediente de crédito se ha utilizado en su contra, el derecho a saber qué figura en su expediente de crédito, el derecho a solicitar su calificación crediticia y el derecho a objetar información incompleta o inexacta. Además, de conformidad con la Ley de Informes de Crédito Justos, las agencias de informes de los consumidores deben corregir o eliminar información inexacta, incompleta o no verificable; las agencias de informes de los consumidores no pueden reportar información negativa obsoleta; el acceso a los expedientes de los consumidores es limitado; los consumidores deben dar su consentimiento para que se proporcionen informes de crédito a los empleadores; los consumidores pueden limitar las ofertas de crédito y de seguro "preseleccionadas" basadas en la información de su informe de crédito; y los consumidores pueden solicitar daños y perjuicios a los infractores. Los consumidores pueden tener derechos adicionales conforme a la Ley de Informes de Crédito Justos, que no figuran aquí. Las víctimas del robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos conforme a la Ley de Informes de Crédito Justos. Le recomendamos que consulte sus derechos conforme a la Ley de Informes de Crédito Justos visitando www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o escribiendo a Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Los residentes de Nueva York pueden comunicarse con el fiscal general de Nueva York en Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

Los residentes de Carolina del Norte pueden comunicarse con el fiscal general de Carolina del Norte en: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 o 1-919-716-6000; y www.ncdoj.gov.

Los residentes de Rhode Island pueden comunicarse con el fiscal general de Rhode Island en: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Según la ley de Rhode Island, las personas tienen derecho a obtener cualquier informe policial presentado con respecto a este evento. Hay aproximadamente <<#>> residentes de Rhode Island que pueden verse afectados por este evento.