

18729



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

Notice of Data Breach

The protection of your personal information is a priority for us at Saint John's School ("Saint John's"). We are writing to inform you of an incident that occurred with one of our vendors, Blackbaud, Inc. ("Blackbaud") which potentially involved your personal information (the "Incident"). We take this matter very seriously, which is why we are offering you the opportunity to activate a complementary identity monitoring service provided by Kroll.

What Happened?

We recently learned that Blackbaud experienced a ransomware security incident. Blackbaud indicated that immediately upon discovery of the Incident, it engaged its cybersecurity team, independent forensics experts, and engaged with law enforcement to investigate and remediate the data security Incident. Immediately upon discovering the Incident, Saint John's engaged in own investigation to determine the scope and extent of Blackbaud's Incident. On November 23, 2020, we determined that the Incident potentially involved unauthorized access of your personal information.

What Information Was Involved?

The personal information that was potentially exposed includes your <<b2b_text_1(Variable Data Elements)>>.

What We Are Doing

We take the security of your personal information seriously. While our investigation confirmed that Blackbaud's Incident did not impact Saint John's systems, we are working to ensure that our vendors implement improved security measures to protect against unauthorized access. Blackbaud indicated that they have implemented several changes that will protect your data from any subsequent incidents. Specifically, Blackbaud's teams were able to quickly identify the vulnerability associated with the Incident, including the tactics used by the cybercriminal, and took swift action to fix it. Additionally, Blackbaud indicated they are accelerating efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

In addition, to help relieve any concerns following the Incident, Saint John's have secured the services of Kroll to provide identity monitoring services at no cost to you for eighteen months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **March 18, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

What You Can Do

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. There is no charge to place, temporarily lift, or permanently remove a security freeze.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

We encourage you to take full advantage of this service offering. Representatives can answer questions or concerns you may have regarding protection of your personal information.

For More Information

If you have questions, please call 1-833-960-3580, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready. Protecting your information is important to Saint John's. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Edwin Rosario

Edwin Rosario
Senior Director – Operations

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Aviso de violación de datos

La protección de su información personal es una prioridad para nosotros en Saint John's School ("Saint John's"). Le escribimos para informarle de un incidente que ocurrió con uno de nuestros proveedores, Blackbaud, Inc. ("Blackbaud") que potencialmente involucró su información personal (el "Incidente"). Nos tomamos este asunto muy en serio, por lo que le ofrecemos la oportunidad de activar un servicio complementario de monitoreo de identidad proporcionado por Kroll.

¿Que pasó?

Recientemente nos enteramos de que Blackbaud experimentó un incidente de seguridad de ransomware. Blackbaud indicó que inmediatamente después del descubrimiento del Incidente, contrató a su equipo de ciberseguridad, expertos forenses independientes y se comprometió con las fuerzas del orden para investigar y remediar el Incidente de seguridad de datos. Inmediatamente después de descubrir el incidente, Saint John's emprendió su propia investigación para determinar el alcance y la extensión del incidente de Blackbaud. El 23 de noviembre de 2020, determinamos que el Incidente potencialmente involucró acceso no autorizado a su información personal.

¿Qué información estuvo involucrada?

La información personal potencialmente expuesta incluye su <<b2b_text_2(Spanish Variable Data Elements)>>.

Qué estamos haciendo

Nos tomamos muy en serio la seguridad de su información personal. Si bien nuestra investigación confirmó que el Incidente de Blackbaud no afectó los sistemas de Saint John's, estamos trabajando para garantizar que nuestros proveedores implementen medidas de seguridad mejoradas para proteger contra el acceso no autorizado. Blackbaud indicó que han implementado varios cambios que protegerán sus datos de incidentes posteriores. Específicamente, los equipos de Blackbaud pudieron identificar rápidamente la vulnerabilidad asociada con el Incidente, incluidas las tácticas utilizadas por el ciberdelincuente, y tomaron medidas rápidas para solucionarlo. Además, Blackbaud indicó que están acelerando los esfuerzos para fortalecer aún más su entorno a través de mejoras en la administración de acceso, segmentación de la red, implementación de terminales adicionales y plataformas basadas en la red.

Además, para ayudar a aliviar cualquier inquietud después del Incidente, Saint John's ha asegurado los servicios de Kroll para brindarle servicios de monitoreo de identidad sin costo para usted durante un año. Kroll es un líder mundial en mitigación y respuesta de riesgos, y su equipo tiene una amplia experiencia en ayudar a personas que han sufrido una exposición involuntaria de datos confidenciales.

Sus servicios de monitoreo de identidad incluyen Monitoreo de Crédito, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, y Identity Theft Restoration.

Visite <https://enroll.idheadquarters.com> para activar y aprovechar sus servicios de monitoreo de identidad.

Tiene hasta el 18 de marzo de 2021 para activar sus servicios de monitoreo de identidad.

Número de membresía: <<Member ID>>

Con esta carta se incluye información adicional que describe sus servicios.

Lo que puedes hacer

Bajo la ley de Massachusetts, usted tiene el derecho de obtener ningún informe policial presentado en relación con este incidente. Si es víctima de un robo de identidad, también tiene derecho a presentar un informe policial y obtener una copia del mismo. La ley de Massachusetts también permite a los consumidores colocar un congelamiento de seguridad en sus informes crediticios. Un congelamiento de seguridad prohíbe que una agencia de informes crediticios divulgue cualquier información del informe crediticio de un consumidor sin autorización escrita. Sin embargo, tenga en cuenta que colocar un congelamiento de seguridad en su informe de crédito puede retrasar, interferir o impedir la aprobación oportuna de cualquier solicitud que realice para nuevos préstamos, hipotecas de crédito, empleo, vivienda u otros servicios. No hay ningún cargo por colocar, levantar temporalmente o eliminar permanentemente un congelamiento de seguridad.

Por favor revise la sección "Recursos adicionales" adjunta incluida con esta carta. Esta sección describe los pasos adicionales que puede tomar para protegerse, incluidas las recomendaciones de la Comisión Federal de Comercio con respecto a la protección contra el robo de identidad y los detalles sobre cómo colocar una alerta de fraude o un congelamiento de seguridad en su archivo de crédito.

Le recomendamos que aproveche al máximo esta oferta de servicios. Los representantes pueden responder preguntas o inquietudes que pueda tener con respecto a la protección de su información personal.

Para más información

Si tiene preguntas, llame al 1-833-960-3580, de lunes a viernes de 8:00 a.m. a 5:30 p.m. Tiempo central. Tenga a mano su número de membresía. La protección de su información es importante para Saint John's. Confiamos en que los servicios que le ofrecemos demuestren nuestro compromiso continuo con su seguridad y satisfacción.

Sinceramente,

Edwin Rosario

Edwin Rosario
Senior Director – Operations

RECURSOS ADICIONALES

La información de contacto de las tres agencias de informes de crédito a nivel nacional es:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Informe de Crédito Gratuito. Se recomienda que permanezca atento a los incidentes de fraude y robo de identidad al revisar los extractos de cuenta y monitorear su informe de crédito para detectar actividades no autorizadas. Puede obtener una copia de su informe de crédito, de forma gratuita, una vez cada 12 meses de cada una de las tres agencias de informes de crédito a nivel nacional.

Para solicitar su informe de crédito anual gratuito, visite www.annualcreditreport.com o llame sin cargo al **1-877-322-8228**.

También puede solicitar su informe de crédito anual gratuito enviando por correo un Formulario de Solicitud de Informe de Crédito Anual completo (disponible en el sitio web de la Comisión Federal de Comercio de los Estados Unidos ("FTC") en www.consumer.ftc.gov) a: Servicio de Solicitud de Informe de Crédito Anual, P.O. Box 105281, Atlanta, GA 30348-5281.

Para los residentes de Colorado, Georgia, Maine, Maryland, Massachusetts, Nueva Jersey, Puerto Rico y Vermont:

Puede obtener una o más (según el estado) copias adicionales de su informe de crédito, sin cargo. Debe comunicarse con cada una de las agencias de informes de crédito directamente para obtener dichos informes adicionales.

Alerta de Fraude. Puede colocar una alerta de fraude en su archivo llamando a una de las tres agencias nacionales de informes de crédito mencionadas anteriormente. Una alerta de fraude le dice a los acreedores que sigan ciertos procedimientos, incluido contactarlo antes de que abran cuentas nuevas o cambien sus cuentas existentes. Por esa razón, colocar una alerta de fraude puede protegerlo, pero también puede retrasarlo cuando busca obtener crédito.

Congelación de Seguridad. Tiene la capacidad de colocar una congelación de seguridad en su informe de crédito.

Un congelamiento de seguridad está destinado a evitar que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. Para congelar la seguridad en su informe de crédito, puede utilizar un proceso en sitio web, una línea telefónica automatizada o una solicitud por escrito a cualquiera de las tres agencias de informes de crédito mencionadas anteriormente. Se debe incluir la siguiente información al solicitar una congelación de seguridad (tenga en cuenta que si solicita un informe de crédito para su cónyuge, esta información también se debe proporcionar para él / ella): (1) nombre completo, con inicial del segundo nombre y cualquier sufijo; (2) número de seguro social; (3) fecha de nacimiento; (4) dirección actual y cualquier dirección anterior de los últimos cinco años; y (5) cualquier informe de incidente aplicable o que cumpla con una agencia de aplicación de la ley o el Registro de Vehículos Motorizados. La solicitud también debe incluir una copia de una tarjeta de identificación emitida por el gobierno y una copia de una factura reciente o un extracto bancario o de seguro. Es esencial que cada copia sea legible, muestre su nombre y dirección postal actual, y la fecha de emisión.

Comisión Federal de Comercio y Fiscalías Generales. Si cree que es víctima de robo de identidad o tiene motivos para creer que su información personal ha sido mal utilizada, debe comunicarse de inmediato con la Comisión Federal de Comercio y / o la oficina del Fiscal General en su estado de origen. También puede comunicarse con estas agencias para obtener información sobre cómo prevenir o evitar el robo de identidad.

Puede comunicarse con la **Comisión Federal de Comercio**, Centro de Respuesta al Consumidor, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Para residentes de Maryland: Puede comunicarse con la Oficina del Fiscal General de Maryland, División de Protección al Consumidor, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

Para residentes de Carolina del Norte: Puede comunicarse con la Oficina del Fiscal General de Carolina del Norte, División de Protección al Consumidor, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Para residentes de Nueva York: Se puede contactar al Fiscal General en: Oficina del Fiscal General, Capitolio, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

Para residentes de Connecticut: Puede comunicarse con la Oficina del Fiscal General de Connecticut, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

Denuncia de robo de identidad y obtención de denuncia policial.

Para los residentes de Iowa: se le aconseja informar cualquier sospecha de robo de identidad a la policía o al Fiscal General de Iowa.

Para los residentes de Massachusetts: tiene derecho a obtener un informe policial si es victorioso del robo de identidad.

Para los residentes de Oregon: se le recomienda informar cualquier sospecha de robo de identidad a las fuerzas del orden público, a la Comisión Federal de Comercio y al Fiscal General de Oregon.

APROVECHE SUS SERVICIOS DE MONITOREO DE IDENTIDAD

Kroll le ha brindado acceso a los siguientes servicios:

Monitoreo de crédito de oficina única (Single Bureau Credit Monitoring)

Recibirá alertas cuando haya cambios en sus datos de crédito, por ejemplo, cuando se solicite una nueva línea de crédito en su nombre. Si no reconoce la actividad, tendrá la opción de llamar a un especialista en fraude de Kroll, que puede ayudarlo a determinar si es un indicador de robo de identidad.

Web Watcher

Observador de Web monitorea los sitios de Internet donde los delincuentes pueden comprar, vender e intercambiar información de identidad personal. Se generará una alerta si se encuentra evidencia de su información de identidad personal.

Public Persona

Persona pública monitorea y notifica cuando los nombres, los alias y las direcciones se asocian con su número de Seguro Social. Si se encuentra información, recibirá una alerta.

Quick Cash Scan

Escaneo rápido de efectivo monitorea las fuentes de préstamos a corto plazo y adelantos en efectivo. Recibirá una alerta cuando se informe un préstamo, y puede llamar a un especialista en fraude de Kroll para obtener más información.

\$1 Million Identity Fraud Loss Reimbursement

Le reembolsa los gastos de su bolsillo por un total de hasta \$ 1 millón en costos legales cubiertos y gastos por cualquier evento de identidad robado. Toda la cobertura está sujeta a las condiciones y exclusiones de la política:

Fraud Consultation

Tiene acceso ilimitado a consultas con un especialista en fraude de Kroll. El soporte incluye mostrarle las formas más efectivas para proteger su identidad, explicar sus derechos y protecciones bajo la ley, asistencia con alertas de fraude e interpretar cómo se accede y utiliza la información personal, incluida la actividad sospechosa de investigación que podría estar vinculada a un evento de robo de identidad.

Identity Theft Restoration

Si resulta ser víctima de un robo de identidad, un investigador experto autorizado de Kroll trabajará en su representación para resolver cualquier problema relacionado. Tendrá acceso a un investigador especializado que entiende sus problemas y que puede realizar la mayor parte del trabajo por usted. Su investigador puede investigar a fondo para revelar todos los aspectos del robo de identidad y luego trabajar para resolverlo.