EXHIBIT 1

By providing this notice, Miami Management Inc. (“Miami Management”) located at 11770 US Highway One, Suite 501, Palm Beach Gardens, FL 33408, does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 10, 2025, Miami Management identified suspicious activity within its network systems. Upon identifying the suspicious activity, Miami Management took steps to ensure the security of the systems and began an investigation with assistance from cybersecurity specialists. The investigation determined that an unknown actor accessed certain systems between September 8, 2025, and October 9, 2025, and viewed or copied certain files. Miami Management undertook a thorough review of the files impacted to determine what information was involved and to whom it relates for the purpose of providing notifications which was completed recently.

The information that could have been subject to unauthorized access includes name, driver's license number, and Social Security number.

Notice to Nebraska Residents

On or about February 2, 2026, Miami Management provided written notice of this incident to three (3) Nebraska 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, Miami Management moved quickly to investigate and respond to the incident, assess the security of Miami Management systems, and identify potentially affected individuals. Miami Management is also working to implement additional safeguards and training to its employees. Miami Management is providing access to credit monitoring services for twelve (12), through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Miami Management is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Miami Management 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.

Miami Management 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

Miami Management Inc.

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

NOTICE OF <<VARIABLE DATA 1>>

Dear <<Full Name>>:

Miami Management Inc. ("Miami Management"), writes to inform you of an event that may impact some of your information. Miami Management takes this event and the privacy, security, and confidentiality of information in our care very seriously. Out of an abundance of caution, we are providing you with information about the event, our response, and resources available to you to help further protect your information, should you feel it necessary to do so.

What Happened? On September 10, 2025, Miami Management identified suspicious activity within its network systems. Upon identifying the suspicious activity, Miami Management took steps to ensure the security of the systems and began an investigation with assistance from cybersecurity specialists. The investigation determined that an unknown actor accessed certain systems between September 8, 2025, and October 9, 2025, and viewed or copied certain files. Therefore, Miami Management undertook a thorough review of the files impacted to determine what information was involved and to whom it relates for the purpose of providing notifications. This review concluded recently and determined that some of your information was within the impacted data.

What Information Was Involved? The review identified the following information associated with you: name, <<Breached Elements>>. Please note, we are not aware of any fraud or misuse of any information in relation to this event.

What We Are Doing. Miami Management takes this event seriously and the privacy, security, and confidentiality of information in our care is among our highest priorities. Upon identifying the suspicious activity, Miami Management moved quickly to ensure the security of our systems and began an investigation. As part of our ongoing commitment to information security, we are currently reviewing our policies, procedures, and security tools to reduce the likelihood of a similar event from occurring in the future. As an added precaution, we are offering you access to <<CM Duration>> months of complimentary identity protection and credit monitoring services through Epiq. More information about these services, including enrollment details, may be found in the *Steps You Can Take to Help Protect Your Personal Information* section of this notice.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may enroll in the offered complimentary identity protection and credit monitoring services. Although we are making these services available to you, we are unable to enroll you directly for privacy reasons. Additional information and resources may be found below in the *Steps You Can Take to Help Protect Your Personal Information* section of this notice.

For More Information. If you have any questions regarding the event, please contact our toll-free phone number at 1-877-421-8528 Monday through Friday from 9am - 9pm Eastern Time.

Sincerely,

Miami Management Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services

<<Full Name>>
Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: <<CM Duration>> Months

Epiq - Privacy Solutions ID
1B Credit Monitoring - Plus

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score and Report[1]
1-Bureau VantageScore® 3.0 (annual) and 1-Bureau Credit Report.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[2]
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[2]
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Plus, please call directly at **866.675.2006,** Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

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; 1-202-442-9828; and oag.dc.gov.

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 Count>> Rhode Island residents that may be impacted by this event.

Miami Management Inc. ("Miami Management") le escribe para informarle sobre un evento que puede afectar parte de su información. Miami Management toma muy en serio este evento, así como la privacidad, seguridad y confidencialidad de la información bajo nuestro cuidado. Por precaución, le proporcionamos información sobre el evento, nuestra respuesta y los recursos disponibles para ayudarle a proteger su información, si considera necesario hacerlo.

¿Qué ocurrió? El 10 de septiembre de 2025, Miami Management identificó actividad sospechosa dentro de sus sistemas de red. Al detectar esta actividad, Miami Management tomó medidas para asegurar los sistemas y comenzó una investigación con la asistencia de especialistas en ciberseguridad. La investigación determinó que un actor desconocido accedió a ciertos sistemas entre el 8 de septiembre de 2025 y el 9 de octubre de 2025, y visualizó o copió ciertos archivos. Por lo tanto, Miami Management realizó una revisión exhaustiva de los archivos afectados para determinar qué información estaba involucrada y a quién correspondía, con el propósito de proporcionar notificaciones. Esta revisión concluyó recientemente y determinó que parte de su información estaba dentro de los datos afectados.

¿Qué información estuvo involucrada? La revisión identificó la siguiente información asociada con usted: nombre, <<Variable Data 2>>. Tenga en cuenta que no tenemos conocimiento de ningún fraude o uso indebido de la información en relación con este evento.

¿Qué estamos haciendo? Miami Management toma este evento muy en serio y la privacidad, seguridad y confidencialidad de la información bajo nuestro cuidado es una de nuestras más altas prioridades. Al identificar la actividad sospechosa, Miami Management actuó rápidamente para asegurar nuestros sistemas e inició una investigación. Como parte de nuestro compromiso continuo con la seguridad de la información, actualmente estamos revisando nuestras políticas, procedimientos y herramientas de seguridad para reducir la probabilidad de que ocurra un evento similar en el futuro. Como medida adicional de precaución, le ofrecemos acceso a 12 meses de servicios gratuitos de protección de identidad y monitoreo de crédito a través de Epiq. Puede encontrar más información sobre estos servicios, incluidos los detalles de inscripción, en la sección **Pasos que Puede Tomar para Ayudar a Proteger su Información Personal** de este aviso.

¿Qué puede hacer usted? Le recomendamos permanecer atento a incidentes de robo de identidad y fraude revisando sus estados de cuenta y monitoreando sus informes de crédito gratuitos para detectar actividad sospechosa o errores. Puede inscribirse en los servicios gratuitos de protección de identidad y monitoreo de crédito ofrecidos. Aunque ponemos estos servicios a su disposición, no podemos inscribirlo directamente por razones de privacidad. Puede encontrar información adicional y recursos más abajo en la sección **Pasos que Puede Tomar para Ayudar a Proteger su Información Personal**.

Para más información. Si tiene alguna pregunta sobre este evento, comuníquese con nuestro número telefónico gratuito al 1-877-421-8528 de lunes a viernes de 9 a.m. a 9 p.m. (hora del Este)

Atentamente,

Miami Management Inc.

Pasos que Puede Tomar para Proteger su Información Personal

Inscríbase en los Servicios de Monitoreo

<<Full Name>>
Código de Activación: <<ACTIVATION CODE>>
Fecha límite de inscripción: <<Variable Data 4>>
Duración de la cobertura: <<CM Duration>> Months

Epiq - Privacy Solutions ID
Monitoreo de Crédito 1B - Plus

Cómo inscribirse:

1) Visite **www.privacysolutionsid.com** y haga clic en "Activate Account"
2) Ingrese el siguiente código de activación, **<<Activation Code>>** y complete el formulario de inscripción
3) Complete el proceso de verificación de identidad
4) Recibirá un correo electrónico separado de **noreply@privacysolutions.com** confirmando que su cuenta ha sido configurada correctamente. Este correo incluirá un enlace **"Access Your Account" (Acceder a su cuenta)** que lo dirigirá a la página de inicio de sesión
5) Ingrese sus credenciales de inicio de sesión
6) Será dirigido a su panel de control y ¡la activación estará completa!

Funciones:

Monitoreo de crédito de 1 buró con alertas
Monitorea su archivo de crédito para detectar cambios importantes, con alertas como consultas de crédito, nuevas cuentas y registros públicos.
Puntaje y reporte de crédito VantageScore® 3.0
1 buró VantageScore® 3.0 (anual) y reporte de crédito de 1 buró.
Monitoreo del SSN (transacciones de alto riesgo, alertas de autenticación e investigaciones en tiempo real)
Detecta y previene eventos comunes de robo de identidad fuera de su informe crediticio. Monitoreo en tiempo real del SSN en situaciones como solicitudes de préstamos, empleo, registros médicos, declaraciones de impuestos, firmas de documentos en línea y plataformas de pago, con alertas.
Monitoreo de la Dark Web
Escanea millones de servidores, salas de chat, foros y sitios web en toda la web para detectar el uso fraudulento de su información personal, con alertas.
Monitoreo de cambio de dirección
Monitorea la base de datos nacional de cambio de dirección (NCOA) y los registros del Servicio Postal de EE. UU. para detectar cambios no autorizados en direcciones actuales o anteriores.
Protección de crédito
Asistencia para congelar la seguridad crediticia en los 3 burós, bloqueando el acceso a su archivo crediticio para otorgar crédito (con ciertas excepciones).
Protección de información personal
Ayuda a encontrar su información personal expuesta en la web pública, específicamente en sitios de búsqueda de personas y corredores de datos, para que pueda optar por eliminarla. Ayuda a proteger contra robo de identidad, llamadas automáticas, acosadores y otros riesgos de privacidad.
Restauración de identidad y asistencia por pérdida de billetera
Especialistas dedicados en restauración de identidad que ayudan con la recuperación tras robo de identidad y con la cancelación y reemisión de tarjetas de crédito e identificación.
Seguro contra robo de identidad hasta $1 millón
Proporciona hasta $1,000,000 (sin deducible) en reembolso de gastos por robo de identidad, basado en el descubrimiento. Este seguro ayuda a cubrir gastos normalmente asociados con el robo de identidad.
Transferencias electrónicas de fondos no autorizadas (UEFT)
Proporciona hasta $1,000,000 (sin deducible) de reembolso por transferencias electrónicas de fondos no autorizadas, ayudando a recuperar fondos robados debido a actividades fraudulentas (basado en ocurrencia).

Si necesita ayuda con el proceso de inscripción o tiene preguntas sobre Epiq – Privacy Solutions ID Monitoreo de Crédito 1B - Plus, llame directamente al **866.675.2006**, de lunes a viernes de 9:00 a.m. a 5:30 p.m., hora del Este.

Los puntajes de crédito proporcionados se basan en el modelo VantageScore® 3.0. Para puntajes de crédito de tres burós, se utilizan datos de Equifax®, Experian® y TransUnion®. Terceros utilizan diferentes tipos de puntajes para evaluar su solvencia crediticia.

El seguro contra robo de identidad está suscrito por subsidiarias o afiliadas de American International Group, Inc. o American Bankers Insurance Company of Florida (una compañía de Assurant). Esta descripción es solo un resumen informativo y no incluye todos los términos, condiciones y exclusiones. Consulte las pólizas reales para detalles. La cobertura puede no estar disponible en todas las jurisdicciones.

Monitoree sus Cuentas

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

Los consumidores tienen derecho a colocar una "alerta de fraude" inicial o extendida en su archivo de crédito sin costo alguno. Una alerta inicial de fraude dura un año. Cuando una empresa ve una alerta de fraude, debe tomar medidas para verificar la identidad del consumidor antes de otorgar nuevo crédito. Si los consumidores son víctimas de robo de identidad, tienen derecho a una alerta de fraude extendida, que dura siete años. Para colocar una alerta de fraude, comuníquese con cualquiera de las agencias de crédito indicadas a continuación.

Como alternativa a una alerta de fraude, los consumidores tienen derecho a colocar un "congelamiento de crédito" en su informe de crédito, lo que prohibirá que una agencia de crédito divulgue información sin la autorización expresa del consumidor. Un congelamiento de crédito está diseñado para evitar que se aprueben créditos, préstamos o servicios a nombre del consumidor sin su consentimiento. Sin embargo, tenga en cuenta que un congelamiento de crédito puede retrasar o interferir con la aprobación de solicitudes futuras de crédito, préstamos o hipotecas. Según la ley federal, no se puede cobrar por colocar o levantar un congelamiento de crédito. Para solicitar un congelamiento, es posible que deba proporcionar:

- Nombre completo (incluyendo segundo nombre e inicial, Jr., Sr., II, III, etc.)
- Número de Seguro Social
- Fecha de nacimiento
- Direcciones de los últimos dos a cinco años
- Comprobante de domicilio actual (factura de servicios públicos o teléfono)
- Copia legible de una identificación emitida por el gobierno
- Copia de un informe policial o denuncia si es víctima de robo de identidad

Contacto de las Agencias de Crédito

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

(Direcciones postales de alertas de fraude y congelamientos de crédito se mantienen igual que en inglés.)

Información Adicional

Los consumidores pueden informarse sobre robo de identidad, alertas de fraude, congelamientos de crédito y pasos para proteger su información personal comunicándose con las agencias de crédito, la Comisión Federal de Comercio (FTC) o el Fiscal General de su estado. La FTC puede contactarse en: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-438-4338; TTY: 1-866-653-4261. La FTC recomienda presentar una queja si descubre que su información ha sido utilizada indebidamente. Los consumidores tienen derecho a presentar un informe policial si experimentan robo de identidad o fraude. Este aviso no ha sido retrasado por las autoridades.(Sección de derechos específicos por estado: Distrito de Columbia, Maryland, Nuevo México, Nueva York, Carolina del Norte y Rhode Island se mantiene igual en estructura, solo traducida.)

Para los residentes del *Distrito de Columbia*, se puede contactar al Fiscal General del Distrito de Columbia en: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; y oag.dc.gov.

Para los residentes de *Nueva York*, se puede contactar al Fiscal General de Nueva York en: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; o https://ag.ny.gov.

Para los residentes de *Carolina del Norte*, se puede contactar al 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.

Para los residentes de *Rhode Island*, se puede contactar al Fiscal General de Rhode Island en: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; y 1-401-274-4400. Conforme a la ley de Rhode Island, las personas tienen derecho a obtener cualquier informe policial presentado con respecto a este evento. Aproximadamente <<Rhode Island Count>> residentes de Rhode Island pueden verse afectados por este evento.