WILSON ELSER

WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

July 9, 2014

Attorney General Joseph Foster
NH Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Foster:

We represent TotalBank with respect to a recent security incident involving the potential exposure of certain personally identifiable information described in more detail below. TotalBank provided notification of this event to its customers in compliance with Gramm-Leach-Bliley Act, and is providing you with this letter in compliance with state notification requirements.

TotalBank is a local bank located in South Florida, Miami, primarily serving the local community. TotalBank takes the security of the information in its control very seriously. Accordingly, it has identified individuals whose personally identifiable information may have been exposed in the incident, discussed below, and provided appropriate services to them including credit monitoring, identity theft protection for one year, and access to fraud resolution representatives.

1. Nature of security incident.

In late May, TotalBank discovered that an unauthorized individual obtained access to its computer network. Based on that discovery they engaged outside data forensic experts to conduct an investigation. Initially, TotalBank believed the intrusion was limited to its wire transfer system. However, on June 24, 2014, they learned that unauthorized individuals may have obtained access to personal information, which includes name, address, account number, account balance, and personal identification number (for example, Social Security number, driver's license number, passport number, Alien Registration number). The information did not include customer passwords or the type of information that would allow access to any bank account. TotalBank's customer accounts remain secure.

2. **Number of New Hampshire residents affected.**

Twelve (12) New Hampshire residents were affected by the security incident. Notification letters to these individuals were mailed on July 03, 2014 via regular mail. A copy of the notification letter is included

with this letter.

3. **Steps you have taken or plan to take relating to the incident.**

As soon as TotalBank discovered the security incident, it cut off access to the impacted computer systems and hired independent computer forensic experts to conduct an investigation. TotalBank also contacted law enforcement, and is cooperating with their investigation.

TotalBank has taken extensive action to strengthen its IT security. This includes reinforcing its internal security protections and firewalls, enhanced threat detection and monitoring, and shutting down access to any compromised system. This is in addition to security measures that were already in place, such as network monitoring, access control lists (ACLs), and tracked authentication.

TotalBank also contracted with identity theft protection experts AllClear ID to provide credit monitoring and identity theft protection to impacted individuals at no cost to individuals for one year. Notice is also being provided to the credit reporting agencies.

4. Contact information.

TotalBank remains dedicated to the protection of the information in its systems. If you have any additional questions, please contact me at Melissa.Ventrone@wilsonelser.com, or (312) 821-6105.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Melissa K. Ventrone

Enclosure

cc: Kevin M Scott

TOTALBANK

Processing Center · P.O. Box 3825 · Suwanee, GA 30024

John Q. Sample
123 Fake St.
Apt. 22
Austin, TX 78701

July 3, 2014

Dear John Q. Sample,

We are writing to inform you of a recent computer security incident at TotalBank that may have resulted in the disclosure of information related to you or your personal or business accounts. We take the security of your personal information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

We recently discovered that an unauthorized individual obtained access to our computer network. Based on that discovery we engaged outside data forensic experts to conduct an investigation. On June 24, 2014, we learned that unauthorized individuals may have obtained access to your personal information which includes your name, address, account number, account balance, and personal identification number (for example, social security number, driver's license number, passport number, alien registration number). The information did not include customer passwords or the type of information that would allow access to your bank account, which remains secure.

We want to assure you that we have reinforced our internal security protections and firewalls, enhanced threat detection and monitoring, and shut down access to any compromised system. We are also continuing to work closely with law enforcement. As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months:

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. This protection is automatically available to you with no enrollment required. If a problem arises, simply call 855-731-6014 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring. For a child under 18 years old, AllClear ID ChildScan identifies fraud by searching various databases for evidence of misuse of the child's information. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 855-731-6014 using the following redemption code: 9999999999.

Please note: Additional steps may be required by you in order to activate your phone alerts.

In addition to the steps we are taking, as always, you should remain vigilant and contact us if you become aware of any suspicious or unauthorized activity.

We deeply regret any inconvenience or concern that this matter may cause you, and remain dedicated to protecting your information.

Sincerely,

Luis de la Aguilera
President and CEO

TOTALBANK

Processing Center · P.O. Box 3825 · Suwanee, GA 30024

John Q. Sample
123 Fake
Apt. 22
Austin, TX 78701

3 de Julio de 2014

Estimado/a John Q. Sample,

Nos dirigimos a usted para informarle de un reciente incidente de seguridad informática en TotalBank que pudiera haber dado lugar a la divulgación de su información personal, o de sus cuentas particulares o de negocios. Para nosotros la seguridad y confidencialidad de su información es un asunto de vital importancia y por ello le expresamos nuestras más sinceras disculpas por cualquier inconveniente que este incidente le pudiera causar. En esta carta, encontrará información sobre los pasos que puede seguir para proteger sus datos, además de los recursos que ponemos a su disposición para ayudarle.

Recientemente conocimos que alguien sin autorización obtuvo acceso a nuestra red informática. Como consecuencia de ello convocamos a expertos externos en el área de seguridad informática para llevar a cabo una investigación a fondo de lo ocurrido. El día 24 de junio de 2014 nos fue comunicado que individuos sin autorización podrían haber obtenido acceso a su información personal, lo cual incluye su nombre, dirección, número de cuenta, saldo de cuenta y números de identificación personal (como número de seguridad social, licencia de conducir, pasaporte o número de registro de extranjero). Dicha información no incluye las contraseñas de los clientes u otro tipo de información que les permita el acceso a su cuenta bancaria, la cual sigue siendo segura.

Podemos garantizarle que hemos reforzado nuestras protecciones internas de seguridad y "firewalls", mejorando el seguimiento y la detección de potenciales amenazas y el bloqueo del acceso a cualquier sistema que haya podido resultar afectado. Además, seguiremos trabajando de forma cercana con las autoridades.

Como medida preventiva adicional, sin costo alguno para usted, hemos acordado que **AllClear ID** proteja su información por 12 meses. Dicho servicio de protección de identidad está disponible a partir de la fecha de esta comunicación y usted podrá utilizarlo en cualquier momento durante los próximos 12 meses:

AllClear SECURE: El equipo de AllClear ID está a su disposición si usted requiere ayuda para proteger su identidad. Esta protección está automáticamente disponible para usted y no necesita registrarse. Si surgiese algún inconveniente, sólo tiene que llamar al número 855-731-6014 y un investigador especializado realizará la labor de recuperar pérdidas financieras, restaurar su crédito y asegurarse de reestablecer adecuadamente su identidad. AllClear mantiene una calificación A+ por el Better Business Bureau.

AllClear PRO: Este servicio ofrece capas adicionales de protección que incluyen el seguimiento y supervisión de crédito. En el caso de menores de 18 años, AllClear ID ChildScan puede identificar fraudes al buscar evidencias de uso inapropiado de información del menor en diversas bases de datos. Para hacer uso del servicio PRO, deberá suministrar su información personal a AllClear ID. Puede suscribirse al servicio a través de la dirección enroll.allclearid.com o por teléfono, llamando al 855-731-6014 utilizando el siguiente código: 9999999999.

Por favor tome en cuenta que la activación de alertas telefónicas puede requerir pasos adicionales.

Adicionalmente a las medidas que estamos tomando, como es usual, usted debe estar atento y contactar a TotalBank si nota alguna actividad sospechosa o no autorizada en sus cuentas.

Lamentamos cualquier inconveniente que este incidente pueda haberle causado y le informamos que seguimos dedicados a proporcionarle la mejor protección posible de su información personal y la de sus cuentas.

Atentamente,

Luis de la Aguilera
Presidente y Consejero Delegado

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

The next 2 paragraphs are regarding incidents involving personal health information. Disregard if not applicable to your situation.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the Califomia Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Fraud Alerts: There are also two types of fraud alerts that 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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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 calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

Información sobre la prevención del robo de identidad

Recomendamos que periódicamente revise los estados de sus cuentas y que obtenga su informe de crédito de una o más de las compañías nacionales de informes de crédito. Puede obtener una copia gratis de su informe de crédito en línea en www.annualcreditreport.com, llamando gratis al 1-877-322-8228, o enviando un Formulario de Solicitud de Informe De crédito Anual (disponible en www.annualcreditreport.com) a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. También puede comprar una copia de su informe de crédito si se comunica con una o más de las tres entidades nacionales de informes de crédito listadas a continuación.

Equifax, P.O. Box 105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

Cuando usted recibe sus informes de crédito, léalos detenidamente. Busque cuentas o consultas de acreedores que usted no inició o no reconoce. Busque información, tal como la dirección y el número del Seguro Social que no sea correcta. Si ve algo que no entiende, llame al número de teléfono que aparece en el informe de la entidad de informes de créditos.

Le recomendamos que mantenga su vigilancia con respecto a la evaluación de los estados de cuentas e informes de crédito y que informe inmediatamente cualquier actividad sospechosa o sospecha de robo de identidad a las autoridades policiales correspondientes, que incluye a la policía local, la oficina del fiscal de su estado y/o la Comisión Federal de Comercio (FTC por sus siglas en inglés). Se puede comunicar con la Comisión Federal de Comercio o la autoridad reguladora de su estado para obtener información adicional sobre cómo evitar el robo de identidad.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Para residentes de Maryland: También puede obtener información sobre cómo prevenir y evitar el robo de la identidad de la Oficina del Fiscal General de Maryland:

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

Para residentes de Massachusetts: También tiene el derecho a obtener un informe policial.

Para residentes de Carolina del Norte: También puede obtener información sobre cómo prevenir y evitar el robo de la identidad de la Oficina del Fiscal General de Carolina del Norte:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Los próximos dos párrafos tienen que ver con incidentes que incluyen información médica personal. Ignorar si no se aplica a su situación.

Recomendamos que periódicamente revise el estado de cuenta de la explicación de beneficios que recibe de su compañía de seguros. Si ve algún servicio que le parece no recibió, por favor comuníquese con la compañía de seguros llamando al número que aparece en el estado de cuenta. Si no recibe estados de cuenta de la explicación de beneficios periódicamente, llame a su proveedor y pídale que le envíen dichos estados luego de proveerle los servicios a su nombre o número.

Puede pedir copias de sus informes de crédito y verificar si hay facturas médicas que no reconoce. Si encuentra algo sospechoso, llame a la entidad de informes de crédito al número de teléfono que aparece en el informe. Guarde una copia de esta notificación para sus archivos en caso de problemas futuros con sus registros médicos. También puede solicitar una copia de su registro médico a su proveedor que servirá como base. Si es un residente de California, le sugerimos que visite el sitio Web de la Oficina de Protección de la Privacidad de California en www.privacy.ca.gov para obtener más información sobre su privacidad médica.

Alertas de fraude: Hay dos tipos de alertas de fraude que puede agregar a su informe de crédito que alertan a sus acreedores que podría ser víctima del fraude: una alerta inicial y una alerta extendida. Usted puede solicitar que se incluya una alerta inicial a su informe de crédito si sospecha que ha sido, o está por ser, víctima del robo de identidad. La alerta de fraude inicial permanece en su informe de crédito durante por lo menos 90 días. Puede agregar una alerta extendida a su informe de crédito si ya ha sido víctima del robo de identidad y tiene la prueba documentaria apropiada. La alerta de fraude extendida permanece en su informe de crédito durante siete años. También puede agregar una alerta de fraude a su informe de crédito llamando al número gratis de cualquiera de las tres entidades nacionales de informes de crédito que se listan a continuación.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Congelamientos de crédito (para quienes no son residentes de Massachusetts): Usted podría tener el derecho a poner un congelamiento del crédito, también conocido como congelamiento de seguridad, a su archivo de crédito, para que no se pueda abrir ningún crédito nuevo en su nombre sin el uso de un número de identificación personal (PIN por sus siglas en inglés) que se crea cuando activa un congelamiento. El congelamiento del crédito fue creado para prevenir que entidades potenciales que otorgan un crédito puedan acceder a su informe de crédito sin su consentimiento. Si usted activa un congelamiento del crédito, los acreedores potenciales y otros terceros no podrán acceder a su informe de crédito a menos que usted cancele transitoriamente el congelamiento. Por lo tanto, usar el congelamiento del crédito podría retrasar su posibilidad de conseguir un crédito. Además, puede tener que pagar comisiones para activar, desactivar y/o eliminar un congelamiento del crédito. Las leyes del congelamiento del crédito varían de estado a estado. El costo de activar, desactivar transitoriamente y eliminar el congelamiento del crédito también varía según el estado, generalmente entre $5 y $20 por cada medida en cada entidad de informes de crédito. *Distinto que el alerta del fraude, debe colocar un congelamiento del crédito por separado en su archivo de crédito en cada una de las entidades de informes de crédito.* Debido a que las instrucciones sobre cómo establecer un congelamiento del crédito son diferentes de un estado a otro, por favor llame a las tres entidades principales que preparan informes de crédito que se indican a continuación para obtener más información:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

Usted puede obtener más información sobre los alertas de fraude y congelamiento del crédito si se comunica con la Comisión Federal de Comercio o una de las entidades de informes de crédito listadas más arriba.

Congelamientos de crédito (para quienes son residentes de Massachusetts): La ley de Massachusetts le brinda el derecho a colocar un congelamiento de seguridad a sus informes de crédito. Un congelamiento de seguridad es creado para prevenir que servicios, créditos y préstamos sean aprobados en su nombre sin su consentimiento. Usar un congelamiento de seguridad, sin embargo, podría retrasar su posibilidad de obtener un crédito. Usted puede solicitar que se ponga un congelamiento a su informe de crédito enviando una solicitud a una entidad de informes de crédito por correo certificado, correo nocturno o correo estampillado a la dirección que sigue:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

Distinto que el alerta del fraude, debe colocar un congelamiento del crédito por separado en su archivo de crédito en cada una de las entidades de informes de crédito. Se debe incluir la siguiente información cuando solicita un congelamiento de seguridad (se debe presentar la documentación suya y de su cónyuge cuando congela el informe de crédito de su cónyuge): Nombre completo, con inicial del segundo nombre y cualquier sufijo; número del Seguro Social; fecha de nacimiento (mes, día y año); dirección actual y direcciones anteriores durante los últimos cinco (5) años; y pago correspondiente (si corresponde) o informe del incidente o denuncia ante una entidad policial o el Departamento de Vehículos Automotores. La solicitud también debe incluir una copia de una tarjeta de identificación emitida por el gobierno, como licencia de conducir, tarjeta de identificación militar o del estado y una copia de una factura de servicios públicos, estado de cuenta bancario o del seguro. Cada copia debe ser legible, indicar su nombre y dirección actual y la fecha de emisión (las fechas de los estados deben ser recientes). La empresa de informes de créditos podría cobrar un costo razonable de hasta $5 para poner un congelamiento o desactivar o eliminar el congelamiento, a menos que usted sea una víctima del robo de identidad o un cónyuge de una víctima del robo de identidad y haya presentado un informe policial válido relacionado con el robo de identidad a la empresa de informes de créditos.

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Automatic 12 months of coverage
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077

Términos de uso de AllClear Secure

Si usted es víctima del fraude usando su información personal sin autorización, AllClear ID ayudará a recuperar sus pérdidas financieras y restaurar su identidad. Los beneficios incluyen:

- Cobertura automática durante 12 meses;
- Sin costo alguno para usted, nunca. La compañía participante paga por AllClear Secure.

Servicios provistos
Si usted sospecha el robo de su identidad, simplemente llame a AllClear ID para presentar una reclamación. AllClear ID proveerá los servicios necesarios y apropiados de resolución ("Servicios") para ayudar a restaurar sus cuentas comprometidas y su identidad según el estado previo al incidente de fraude. Los servicios son determinados a entera discreción de AllClear ID y están sujetos a los términos y condiciones que se indican en el sitio Web de AllClear ID. AllClear Secure no es una póliza de seguros y AllClear ID no realizará pagos ni reembolsos por pérdidas financieras, obligaciones o gastos que usted incurra.

Período de cobertura
Usted está automáticamente protegido durante 12 meses desde la fecha en que ocurrió el incidente, según se indica en la carta de notificación de incidente que recibió de la empresa (el "Período de Cobertura"). Los eventos de fraude que ocurrieron antes de su Período de cobertura no están cubiertos por los servicios de AllClear Secure.

Requisitos de participación
Para cumplir los requisitos de los Servicios bajo la cobertura de AllClear Secure, debe cumplir totalmente, sin limitaciones, con sus obligaciones según los términos de la presente, debe ser un ciudadano o residente legal, tener (18) años de edad o más, residir en los Estados Unidos y tener un número válido del Seguro Social de EE.UU. Las personas menores de dieciocho (18) años podrían cumplir los requisitos pero deben ser patrocinados por un padre o tutor. Los Servicios solamente lo cubren a usted y a sus cuentas personales médicas y financieras que estén directamente asociadas con su número válido del Seguro Social, incluyendo pero sin limitación a cuentas de tarjetas de crédito, bancarias u otras cuentas financieras y/o cuentas médicas.

Cómo presentar una reclamación
Si usted es víctima de un fraude cubierto por AllClear Secure, debe:

- Notificar a AllClear ID llamando al 1.855.434.8077 para reportar el fraude antes del vencimiento de su Período de cobertura;
- Presentar una prueba de elegibilidad de AllClear Secure al proveer el código de rescate de la carta de notificación que recibió de la Compañía patrocinante;
- Cooperar total y verazmente con AllClear ID sobre el Evento y aceptar presentar cualquier documento que AllClear ID pudiera razonablemente requerir;
- Cooperar totalmente con AllClear ID en cualquier proceso de resolución, que incluye pero no se limita a, presentar a AllClear ID copias de todos los informes o archivos disponibles de la investigación de cualquier institución, que incluye pero no se limita a, instituciones crediticias o departamentos de policía, relacionados con el supuesto robo.

La cobertura bajo AllClear Secure no se aplica a lo siguiente:
Cualquier gasto, daño o pérdida:

- Debido a
  - Cualquier transacción en sus cuentas financieras hechas por usuarios autorizados, incluso si actúan sin su conocimiento
  - Cualquier acto de robo, engaño, confabulación, deshonestidad o criminal suyo o de cualquier persona que actúa junto con usted o por cualquiera de sus representantes autorizados, actúen por cuenta propia o conjuntamente con usted u otros (conjuntamente, su "Falsificación")
- Incurrido por usted de un Evento que no ocurrió durante el período de cobertura;
- Relacionado con un Evento que usted no reporta a AllClear ID antes del vencimiento del período de cobertura de AllClear Secure.

Otras exclusiones:

- AllClear ID no pagará ni tendrá ninguna obligación ante ninguno de los costos o gastos excepto los que se describen en la presente, incluyendo pero sin limitación, honorarios de proveedores de servicios no contratados por AllClear ID; AllClear ID se reserva el derecho a investigar cualquier reclamación presentada para determinar su validez;
- AllClear ID no es una compañía de seguros y AllClear Secure no es una póliza de seguro; AllClear ID no realizará pagos ni reembolsos a usted por cualquier pérdida u obligación que pudiera incurrir;
- AllClear ID no es una organización de reparación del crédito, no es un servicio de asesoramiento de crédito y no promete ayudarle a mejorar su historia crediticia o calificación por encima de la resolución de incidentes de fraude; y
- Se espera que proteja su información personal de manera razonable en todo momento. Por lo tanto, usted no divulgará ni publicará su número del Seguro Social o cualquier otra información personal de manera inadecuada a quienes se pudiera esperar razonablemente que usen o divulguen de manera impropia dicha Información Personal, tales como, por ejemplo, como respuesta a "phishing", mensajes electrónicos no solicitados o mensajes instantáneos que tratan de obtener información personal.

Política de rechazo
Si por cualquier razón usted desea que su información sea eliminada de la base de datos de elegibilidad de AllClear Secure, por favor, comuníquese con AllClear ID:

Correo electrónico	Correo	Teléfono
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077