BY ONLINE SUBMISSION

Office of the Attorney General
6 State House Station
Augusta, ME 04333

February 4, 2021

To Whom It May Concern:

On behalf of US Claims Capital ("US Claims"), this letter provides notice of a computer data security incident, pursuant to Me. Rev. Stat. tit. 10, § 1348, affecting 6 residents of your state.

By way of background, US Claims provides pre-settlement funding to individuals with personal injury claims across the nation. US Claims specializes in assisting personal injury victims with mature claims and confirmed insurance.

On December 4, 2020, US Claims learned that an unauthorized third party gained remote access to an employee email account. Upon discovery, US Claims conducted an enterprise-wide password reset, reported the incident to law enforcement, and engaged external cybersecurity experts to assist it in responding to the incident.

Our investigation of the incident has determined that, on or about October 23, 2020, an unauthorized third party accessed a US Claims employee inbox and may have accessed or downloaded certain personal information contained in that inbox. The unauthorized third party also used this access to initiate fraudulent wire requests and send phishing emails to additional US Claims employees and two external partners. In the course of the investigation, US Claims discovered that the unauthorized party accessed two additional employee inboxes on December 4, 2020, shortly before the account passwords were reset. US Claims has also alerted the two external partners, who reported that that they did not click on any links in the emails received from the compromised US Claims account.

On January 12, 2021, after a detailed search that included a manual review of thousands of files, we identified 6 Maine residents whose personal information may have been accessed by the unauthorized party. A number of these affected individuals were customers of US Claims' prior affiliate, DRB Capital, and this is made clear in their notification letters from US Claims. Depending on the individual, the types of information stored in the mailbox may have included the following: name, address, Social Security number, and date of birth. We are not aware of any resulting identity theft, fraud, or financial losses to customers.

US Claims anticipates that it will begin sending these individuals formal notice on or around February 5, 2021via U.S. mail. A sample of the notification letter is enclosed. As stated in the attached sample notice, US Claims is offering to provide individuals 24 months of free identity theft and credit monitoring services through Kroll. We have also established a call center to respond to individuals' questions.

US Claims takes the protection of personal information of all of its customers and employees seriously and is committed to answering any questions that you may have. Please do not hesitate to contact me at iberlingeri@usclaims.com or (561) 982-3242.

Respectfully yours,

Ina Berlingeri-Vincenty
General Counsel

Enclosure

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

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

NOTICE OF <<B2B_TEXT_1(SUBJECTLINE)>>

Dear <<first_name>>,

We are writing to notify you of a security incident that occurred at US Claims involving some of your personal information. We want to make clear at the outset that keeping your information safe and secure is very important to us, and we deeply regret that this incident occurred.

WHAT HAPPENED?

On December 4, 2020 we learned that an unauthorized party had gained remote access to a US Claims employee's inbox for a limited period of time and acquired certain information, potentially including personal information<<b2b_text_2(ClientStatement)>>. We immediately began to investigate and remediate the incident, including taking swift action to eliminate the access and further enhance our security.

WHAT INFORMATION WAS INVOLVED?

<<b2b_text_3(ClientStatement2)>>The information involved includes your <<b2b_text_4(ImpactedDataElements)>>.

We have seen no evidence that your <<b2b_text_5(NonImpactedDataElements)>> was involved in this incident.

WHAT WE ARE DOING

Our security team took prompt steps to address this incident, including contacting law enforcement and engaging third-party cybersecurity experts to assist us in remediating and ensuring the ongoing security of our systems.

We have engaged Kroll to provide two years of identity monitoring services at no cost to you. Your identity monitoring services include Credit Monitoring, Fraud Consultation and Identity Theft Restoration services.

Please visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services. Note that you have until ***<Date>*** to activate your identity monitoring services.

Your membership number to activate is: **<<Member ID>>**.

WHAT YOU CAN DO

We strongly encourage you to contact Kroll and take advantage of the identity monitoring services we are providing to you free of charge. Remain vigilant and carefully review your accounts for any suspicious activity.

If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities.

FOR MORE INFORMATION

If you would like to take additional steps to protect your personal information, attached to this letter are helpful tips on how to do so.

We take our responsibility to protect your information extremely seriously, and we are very sorry for any inconvenience that this has caused you. If you have any questions regarding this incident or the services available to you, additional assistance is available by calling 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

US Claims Capital

Additional Helpful Tips

Helpful Contacts: You can learn more about how to protect your credit by contacting the Federal Trade Commission (FTC) or your state's Attorney General to obtain information including about how to avoid identity theft, place a fraud alert, and place a security freeze on your credit report.

- ***Federal Trade Commission,*** *Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-IDTHEFT (438-5338), www.ftc.gov/idtheft*

Order Your Free Credit Report. To obtain an annual free copy of your credit reports, visit annualcreditreport.com, call toll-free at 1-877-322-8228, or contact the major credit reporting agencies. Their contact information is as follows:

Equifax:	**Experian:**	**TransUnion:**
equifax.com	**experian.com**	**transunion.com**
freeze.equifax.com	**experian.com/freeze**	**transunion.com/freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-888-909-8872

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report at no charge. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent but may delay your ability to obtain credit. To place a security freeze, you must contact each of the three credit bureaus listed above and may be required to provide your full name; SSN; date of birth; the addresses where you have lived over the past five years; proof of current address, such as a utility bill or telephone bill; a copy of a government issued identification card; and if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency.

Fraud or Identity Theft. If you suspect incidents of identity theft, you should file a report to law enforcement, the FTC, or the Attorney General. If you are the victim of fraud or identity, you have the right to (1) notify the police and Attorney General of your state; and (2) to obtain and file a police report relating to this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identify theft victims and active duty military personnel have additional rights. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

State-Specific Notices. Residents of the following states should review the following information:

- **For District of Columbia residents:** You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.
- **For Maryland residents:** You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.
- **For New York residents:** You may contact the Office of the New York Office of the Attorney General, The Capitol, Albany NY 12224-0341, https://www.ag.ny.gov/, 1-800-771-7755.
- **For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226.
- **For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.
- **For Rhode Island residents:** You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, http://www.riag.ri.gov/index.php, (401) 274-4400.
- **For Colorado, Georgia, Maine, Maryland, New Jersey, 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 bureaus directly to obtain such additional copies.

Kroll | A Division of DUFF&PHELPS

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.

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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.