

March 28, 2022

Rachel H Cobble
205.709.8991 (direct)
423.653.9044 (mobile)
Rachel.Cobble@wilsonelser.com

Via electronic-mail: Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Re:	Our Client	:	Rentex, Inc.
	Matter	:	Data Security Incident on September 12, 2021
	Wilson Elser File #	:	16516.1641

Dear Attorney General Frosh:

We represent Rentex, Inc. (hereinafter “Rentex”), located in Canton, Massachusetts, with respect to a data security incident described in more detail below. Rentex takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of Maryland residents being notified, what information has been compromised, and the steps that Rentex is taking to restore the integrity of the system. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On September 12, 2021, Rentex was the target of a cybersecurity incident. An unauthorized third party attempted to infiltrate Rentex’s computer systems. This incident may have resulted in the exposure of personal information that is located on Rentex’s systems, including full name and social security number. This information is maintained consistent with our employer-employee relationship, including standard administrative and payroll functions.

Rentex is not aware of any evidence that information has been misused and has not received any reports of related identity theft since the date of the incident.

2. Number of Maryland Residents Affected

A total of one hundred eleven (111) residents of Maryland were potentially affected by this security incident. Notification letters to these individuals were mailed on February 28, 2022, by first class mail.

3. Steps Taken

Upon learning of this incident, Rentex moved quickly to institute a response plan, which included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to confirm the security of any relevant systems. Rentex has reviewed, altered and enhanced its policies and procedures relating to the security of its systems and servers.

4. Contact Information

Rentex remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Rachel.Cobble@WilsonElser.com or 205.709.8991.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Rachel H. Cobble, Esq.

Copy: Ross Molina, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*

Rentex, Inc.

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-833-903-3648
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

February 25, 2022

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing in order to inform you of an incident that may have exposed some of your sensitive personal information. We take the privacy of your personal information seriously and want to provide you with information and resources you can use to help protect your information.

What Happened

Rentex, Inc. ("Rentex") detected and stopped a network security incident on September 12, 2021. An unauthorized third-party attempted to infiltrate our network. We immediately shut off access to the network and engaged specialized third-party forensic and technical resources to respond to the incident. Rentex has secured and remediated its network and the data we maintain.

What Information Was Involved

Based on the results of the forensic investigation, we have determined that information - including your name and social security number - were potentially accessed by an unknown party that is not authorized to handle or view such information. We maintain this information consistent with our employer-employee relationship, including administrative and payroll functions.

At this time, Rentex does not have any evidence to indicate that any of your personal information has been or will be misused as a result of this incident. Nevertheless, Rentex decided to notify you of this incident out of an abundance of caution.

What We Are Doing

Once our environment was secure, we initiated a comprehensive investigation into the extent of the unauthorized activity. As of this writing, Rentex has not received any reports of related identity theft since the date of the incident.

To help relieve concerns and restore confidence following this incident, we are offering theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.



Rentex Audio Visual & Computer Rentals

Boston | New York/NJ | Philadelphia | Washington D.C. | Orlando | Las Vegas | Dallas/Ft Worth | Chicago | Anaheim/LA | San Francisco

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is May 25, 2022.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please contact IDX using the information above for assistance or for any additional questions you may have.

Sincerely,

Marcus De Luco

Chief Technology Officer
Rentex Inc

(Enclosure)





Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.



6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

