LETTER TO ATTORNEY GENERAL

Date: September 3, 2020

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
Email: SecurityBreach@atg.wa.gov

Dear Attorney General Ferguson:

We are writing to notify you of a data security incident involving 38,523 Washington residents.

We are unaware of any resulting identity theft, fraud, or financial losses to consumers and have implemented technical and organizational measures to address the security incident and prevent further breaches.

TIMELINE OF EVENTS

We, LiveAuctioneers, are a New-York-based company that provides a marketplace for individuals to buy and sell art, antiques, jewelry and collectibles by hosting auctions in real time via the Internet. On June 19, 2020, an unknown hacker (the "**Hacker**") breached one of our third party software solutions. By exploiting this third party software, the Hacker obtained a source control key to gain access to our source controller repository maintained by another third party software developed, our cloud-based storage environment, and our production database. The Hacker used credentials from internal users to connect and download the database of consumer credentials (the "**user database**"), which included user names and hashed passwords of data subjects, and records of past sales transactions (which included general information about the sale but did not include any user financial account information). No other business operations (e.g., HR or CRM systems) were compromised.

On July 10, 2020, user passwords, which are encrypted weekly, were decrypted by the Hacker, then posted along with user names online for sale. At the time of the breach, the following security safeguards were in place at LiveAuctioneers: (i) implementation of a segmented network; (ii) service level security; (iii) web application firewall and Amazon Web Services security group firewall restrictions; and (iv) hashing and encryption of personal information (passwords were encrypted using MD5 encryption standard).

On July 2, 2020, the third party software provider that was the source of the security incident provided us with initial notice that its systems had been compromised. July 11, 2020, the software developer provided us with updated notice that our users' data had been compromised and that the third party observed our users' information for sale online on the dark web. We immediately expired passwords for all user accounts.

On July 11, we provided initial e-mail notice to users who had been active on our platform in the past year and on August 3, 2020, we provided notice to all other users. We also posted each notice on our website detailing the security breach. Among other things, we urged users to:

- Change passwords for any other online accounts for which they used the same or similar password as used for their LiveAuctioneers account;
- Review their accounts for suspicious activity;
- Be cautious of any unsolicited communications asking for your personal information; and
- Avoid clicking on links or downloading attachments from suspicious emails.

On July 15, 2020, we made incident report to FBI. We received a call back from the FBI the next day and provided information to aid their investigation.

We have engaged with outside expert forensic security consultants to determine the scope of the breach, as well as legal counsel.

INFORMATION INVOLVED/NOT INVOLVED

The data accessed was all in electronic form. Specifically, the following data were compromised for at least some user accounts:

- Name
- Email address (user name)
- Password (encrypted to MD5 standard, but later decrypted by Hacker using brute force)
- Contact details (mailing address, phone number)
- IP addresses used to create user account

The following personal information was **never** collected and therefore **not** compromised:

- Gender, date of birth and/or age
- Social Security Number
- Financial data
- (Copies of) passports or other identity documents

STEPS WE HAVE TAKEN RELATING TO THE INCIDENT

Since the incident, we have taken actions to improve security around our user information and to limit the impact of the data breach. For example, we:

- Blocked the unauthorized access to bidder account information, and expired all passwords associated with user accounts immediately upon discovery the breach;
- Implemented stronger encryption protocols for passwords, using the following encryption standard: PBKDF2 using SHA512 w/15,000 iterations and 64 byte salt;
- Are implementing a “salt and hash” password method so the Company will be storing only tokens and not passwords, in accordance with best practice;
- Expired and replaced all security tokens and access keys for various services throughout our solutions;
- Made all system access tokenized so no application code will have any credentials;
- Require 2 factor authentication for all AWS and internal systems;
- Are analyzing and monitoring our source code to address vulnerabilities; and
- Are upgrading our network infrastructure. For example, Company has implemented VPC flow log, has audited and begun restricting security group access, is in process of implementing Guard Duty IDS, is removing all public access (even via firewall) to our databases, and is in process of implementing a new WAF

CONTACT INFORMATION
If you have any additional questions, please contact Gilad Andorn, Director of Finance & Strategy, 10 E 38th Street, New York, NY 10016, email: gilad.andorn@liveauctioneers.com, Phone Number: (312) 409-3450; or Rob Cummings, Chief Technology Officer, 12244 S. Business Park Drive, Suite 115, Draper, UT 84020, email: rob.cummings@liveauctioneers.com, Phone Number: 801-671-0639 if you need any additional information.

For our website notice, please see https://help.liveauctioneers.com/article/496-july-11-2020-liveauctioneers-account-security.

Enclosed, please find the template notices we sent to residents of Washington.

Sincerely,

Phil Michaelson
Title: CEO
Email: phil.michaelson@liveauctioneers.com
Phone Number: 917-282-5791

Dear {{first_name}},

We take the protection of your information very seriously. Unfortunately, we are writing to inform you about a data security issue affecting your LiveAuctioneers bidder account information. We are deeply sorry for any concern or inconvenience this may have caused, and are working quickly to take the appropriate steps to prevent such incidents in the future. We hope that in time we can regain your trust, which we value above all.

What Happened

Our cybersecurity team has indeed confirmed that following a cyber attack against one of our IT suppliers on June 19, 2020, an unauthorised third party managed to access certain personal information from our bidder database. We were notified of the incident on July 11, 2020.

LiveAuctioneers was one of a number of their partners who experienced a breach since this IT supplier's security was compromised. Our cybersecurity team has ensured the unauthorized access has ceased.

What Information Was Involved

The data that has been exposed includes user account information like names, email addresses, mailing addresses, phone numbers, visit history, and encrypted passwords (the unauthorised party however managed to decrypt passwords after the cyber attack). Not all of this information may have been present on your bidder account. Please also know that complete payment card numbers were not accessed, and we have no reason to believe auction history was affected.

The exposure of your LiveAuctioneers credentials (i.e. login and password) could affect other online accounts you may have (if they use the same or similar credentials). You could also be exposed to impersonation and phishing attempts.

What We Are Doing

As soon as we became aware of this incident, we blocked the unauthorised access to bidder account information and disabled your most recent LiveAuctioneers password.

We have taken immediate steps to improve our security and prevent such incidents in the future:

- We have suspended our relationship with the compromised IT supplier.
- Our security tokens and passwords throughout LiveAuctioneers' systems have been replaced.
- We have implemented stronger password encryption.
- We have partnered with leading cyber security experts to further secure our website, mobile apps, and systems.
- We are working with government authorities to bring the perpetrators to justice.
- Multi-factor authentication for all back-end services have been implemented.

- We are analyzing and monitoring our source code to address any vulnerabilities.
- We are continuing to upgrade our network infrastructure.
- We will be implementing stronger password requirements.

What You Can Do
All passwords created before July 11, 2020 have been disabled. If you have not already done so, we encourage you to change your password.

For not logged in bidders: You can access your account by creating a new password, following the steps below:

- Visit https://www.liveauctioneers.com/ and click “Log In” on the top right-hand corner of the page.
- Click “Forgot Password” on the login window.
- Enter your email address used for and click “Send Reset Instructions”.
- Check your email and follow the link provided to reset your password.

For already logged in bidders: Please click the dropdown from your user icon in the top right corner and click “Account Settings”. From here, click “Change Password”.

To help further protect your personal information, please remember:

- Do not use same or similar credentials for other online accounts.
- Change any and all passwords that used the same or similar credentials as those used for your LiveAuctioneers account.
- Regularly review your online accounts for suspicious activity.
- Be cautious of any unsolicited communications asking for your personal information: we will never ask you to disclose your password via an email or over the phone for instance.
- Avoid clicking on links or downloading attachments from suspicious emails.

If you see any unauthorized activity related to your financial accounts, promptly contact your financial institution. We also suggest you submit a complaint with the Federal Trade Commission by calling 1-877-ID-THEFT (1-877-438-4338), online at https://www.ftc.gov, or by mail to 600 Pennsylvania Avenue, NW Washington, DC 20580.

You also may want to monitor your credit reports with the major credit reporting agencies:

Equifax
1-800-685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian
1-888-397-3742
P.O. Box 9701
Allen, TX 75013
www.experian.com

TransUnion
1-800-916-8800
P.O. Box 1000
Chester, PA 19022
www.transunion.com

For further information, please see our updates at: https://help.liveauctioneers.com/article/496-july-11-2020-liveauctioneers-account-security.

If you have any questions or notice anything suspicious on your account, please contact our customer support team at info@liveauctioneers.com. You can also reach us Mon-Fri XAM - XPM EDT, toll-free at TBD.

Protecting your information and preventing incidents like this from happening in the future is our top priority. We will keep working to improve security and rebuild your trust in us.

LiveAuctioneers

[Update for RoW]

Subject line:
Update regarding your account security

Dear valued bidder,

We are reaching out to share the latest updates following the data incident we emailed you about on July 11, 2020.

What Happened

We take data security very seriously. As communicated in our previous message, following a cyber attack against one of our IT suppliers on June 19, 2020, an unauthorised third party managed to access certain personal information from our bidder database. We became aware of the incident on July 11, 2020, and immediately blocked the unauthorised access to bidder account information and disabled all bidder passwords on LiveAuctioneers. That same day, we notified you through email and published a notice on our website (https://help.liveauctioneers.com/article/496-july-11-2020-liveauctioneers-account-security).

We are deeply sorry for any concern or inconvenience this may have caused, and are working quickly to take the appropriate steps to prevent such incidents in the future. We hope that in time we can regain your trust, which we value above all.

What We Are Doing

Since we last reached out to you, we have taken numerous steps to improve our security and prevent such incidents in the future:

- We have suspended our relationship with the compromised IT supplier.
- Our security tokens and passwords throughout LiveAuctioneers' systems have been replaced.
- We have implemented stronger password encryption.
- We have partnered with leading cyber security experts to further secure our website, mobile apps, and systems.
- We are working with government authorities to bring the perpetrators to justice.
- Multi-factor authentication for all back-end services have been implemented.
- We are analyzing and monitoring our source code to address any vulnerabilities.
- We are continuing to upgrade our network infrastructure.
- We will be implementing stronger password requirements.

What Information Was Involved

The data that has been exposed includes user account information like names, email addresses, mailing addresses, phone numbers, visit history, and encrypted passwords (the unauthorised party however managed to decrypt passwords after the cyber attack). Not all of this information may have been present on your bidder account.
Our team has confirmed that complete debit and credit card numbers were not accessed, and we have no reason to believe auction history was affected.

What You Can Do

If you used the same email address and password on LiveAuctioneers to login to other online accounts, then those accounts could be affected. You could also be exposed to impersonation and phishing attempts.

If you see any unauthorized activity related to your financial accounts, promptly contact your financial institution. We also suggest you submit a complaint with the Federal Trade Commission by calling 1-877-ID-THEFT (1-877-438-4338), online at https://www.ftc.gov, or by mail to 600 Pennsylvania Avenue, NW Washington, DC 20580.

You also may want to monitor your credit reports with the major credit reporting agencies:

Equifax
1-800-685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian
1-888-397-3742
P.O. Box 9701
Allen, TX 75013
www.experian.com

TransUnion
1-800-916-8800
P.O. Box 1000
Chester, PA 19022
www.transunion.com

More Information

For further information, please see our updates at: https://help.liveauctioneers.com/article/496-july-11-2020-liveauctioneers-account-security.

If you have any questions or notice anything suspicious on your account, please contact our customer support team at info@liveauctioneers.com.

Protecting your information and preventing incidents like this from happening in the future is our top priority. We will keep working to improve security and rebuild your trust in us.

LiveAuctioneers