

PAUL HASTINGS

1(312) 499-6016
aaroncharfoos@paulhastings.com

October 13, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: Notice of Security Event

To Whom It May Concern:

We represent AvidXchange, Inc. ("AvidXchange") located at 1210 AvidXchange Lane, Charlotte, North Carolina 28206. We write to notify you of a security event that affected the security of certain personal information relating to approximately seventeen (17) Maryland residents. By providing this notice, AvidXchange does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data breach notification statute, or personal jurisdiction.

Nature of the Security Event

On April 3, 2023, AvidXchange detected a cybersecurity incident as part of its routine security monitoring protocols. Upon learning of the incident, AvidXchange launched an investigation with the support of leading cybersecurity experts. Through its investigation, AvidXchange determined that the earliest evidence of unauthorized access was through a third party vendor. Additionally, AvidXchange determined that the incident affected some of AvidXchange's systems and that data from these systems was exfiltrated. Between May 2, 2023, and May 31, 2023, threat actors published several sets of data from the extraction. AvidXchange worked with a third party to review the data, which included internal, non-personally identifiable, corporate information. On September 27, 2023, AvidXchange confirmed that these data sets contained certain categories of personally identifiable information of employees, dependents, and investors. The categories of personally identifiable information include driver's license number, financial account number, credit card information, Social Security number, date of birth, electronic signature, health insurance information, and passport number.

Notice to Maryland Residents

On April 29, 2023, AvidXchange provided an initial public notice of the security event on its website. On May 15, 2023, AvidXchange emailed its business customers and employees to notify them about the incident and the possibility that personally identifiable information may have been included in the data. The email notice to employees included an offer for employees and dependents to enroll in complimentary credit monitoring. On or about October 13, 2023, AvidXchange will provide written notice to affected Maryland residents with an offer to provide complimentary credit monitoring services. Attached to this letter is a template copy of the notice provided to approximately seventeen (17) Maryland residents impacted by the event.

Office of the Attorney General
October 13, 2023
Page 2

Other Steps Taken In Response

Security is a critical concern and priority for AvidXchange, and the company has taken steps to implement additional safeguards and harden its system. These steps include:

- Expanding our threat detection capabilities and internal security protocol;
- Establishing separate, cloud-based user accounts to further limit and restrict the capabilities of privileged accounts;
- Modifying firewall settings to further restrict inbound and outbound access to our environments;
- Implementing additional logging and imposing restrictions to limit access to sensitive systems;
- Updating user access controls to require smart, context-dependent authentication; and
- Deploying a new, highly secured virtual desktop environment.

Should you have any questions regarding this notification or other aspects of this data security event, please do not hesitate to contact us.

Sincerely,

/s/ Aaron Charfoos

Aaron Charfoos
for PAUL HASTINGS LLP

Enclosure



P.O. Box 989728
West Sacramento, CA 95798-9728

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

October 13, 2023

<<Notice of Data Breach>>

Dear <<FIRST NAME>> <<LAST NAME>>,

AvidXchange, Inc. ("AvidXchange") writes to notify you of a recent incident that involved your personal information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it is appropriate to do so.

What Happened

In early April 2023, AvidXchange detected a cybersecurity incident as part of our routine security monitoring protocols. In response to the incident, we launched an investigation with the support of leading cybersecurity experts, reached out to law enforcement, expelled the threat actor from our systems, and accelerated our planned security enhancements. Our investigation revealed that the incident affected some of AvidXchange's systems and that data from these systems was extracted. Further, between May 2, 2023 and May 31, 2023, threat actors published several sets of data from the extraction. These data sets contained confidential information from our files, including personal information. We conducted a manual review of the personal information to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved

The following types of information related to you were extracted without authorization: name and <<Variable Text 1>>.

What We Are Doing

We are protecting your information, as well as customer information, by taking action to implement additional safeguards and harden our systems. These safeguards include: establishing separate, cloud-based user accounts to further limit and restrict the capabilities of privileged accounts; implementing additional logging processes and imposing more restrictions to limit access to sensitive systems; updating user access controls to require smart, context-dependent authentication; modifying firewall settings to further restrict inbound and outbound access to our environments; and deploying a new, highly secured virtual desktop environment. These safeguards are in place today, with many others being actively designed and implemented on an ongoing basis.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> 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 affected as part of this incident.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (888) 861-7014, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is January 13, 2024.

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 call (888) 861-7014 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

AvidXchange, Inc.

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or 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 (888) 861-7014 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. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: the District of Columbia Attorney General, 400 6th Street, NW, Washington, D.C. 20001; oag.dc.gov; Telephone: 1-202-727-3400.

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: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. There are approximately 4 Rhode Island residents that may be impacted by this event.

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

PAUL HASTINGS

1(312) 499-6016
aaroncharfoos@paulhastings.com

December 6, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: Supplemental Notice of Security Event

To Whom it May Concern:

We represent AvidXchange, Inc. ("AvidXchange") located at 1210 AvidXchange Lane, Charlotte, North Carolina 28206. On October 13, 2023, we notified your office of a security event. We write to supplement that prior notice and notify you that the event also affected the security of certain personal information of approximately one Maryland resident whose personal information AvidXchange was processing for one of AvidXchange's business customers ("Client"). By providing this notice, AvidXchange does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data breach notification statute, or personal jurisdiction.

Nature of the Security Event

As we previously explained in our notice to your office on October 13, 2023, AvidXchange detected a cybersecurity incident as part of its routine security monitoring protocols on April 3, 2023. Upon learning of the incident, AvidXchange launched an investigation with the support of leading cybersecurity experts. Through its investigation, AvidXchange determined that the earliest evidence of unauthorized access was through a third party vendor. Ultimately, AvidXchange determined that certain systems were subject to unauthorized access or acquisition between March 2, 2023 and April 27, 2023. Additionally, AvidXchange determined that the incident affected some of AvidXchange's systems and that data from these systems was exfiltrated. Between May 2, 2023, and May 31, 2023, threat actors published several sets of data from the extraction. AvidXchange worked with a third party to review the data, which included internal, non-personally identifiable, corporate information. On September 27, 2023, AvidXchange confirmed that these data sets contained certain categories of personally identifiable information of employees, dependents, and investors. The categories of personally identifiable information include driver's license number, financial account number, credit card information, Social Security number, date of birth, electronic signature, health insurance information, and passport number.

Notice to Maryland Residents

AvidXchange provided notice to Client of this event and offered to notify affected individuals. On or about December 11, 2023, AvidXchange will provide written notice of this event to affected individuals on Client's behalf and at their direction. This mailing includes notice to approximately one Maryland resident impacted by the event who is affiliated with Client.

VIA E-MAIL

Office of the Attorney General
December 6, 2023
Page 2

Other Steps Taken In Response

As we previously explained in our notice to your office on October 13, 2023, security is a critical concern and priority for AvidXchange, and the company has taken steps to implement additional safeguards and harden its system. These steps include:

- Expanding our threat detection capabilities and internal security protocol;
- Establishing separate, cloud-based user accounts to further limit and restrict the capabilities of privileged accounts;
- Modifying firewall settings to further restrict inbound and outbound access to our environments;
- Implementing additional logging and imposing restrictions to limit access to sensitive systems;
- Updating user access controls to require smart, context-dependent authentication; and
- Deploying a new, highly secured virtual desktop environment

Sincerely,

/s/ Aaron Charfoos

Aaron Charfoos
for PAUL HASTINGS LLP

Enclosure

EXHIBIT A



Return to IDX
4145 SW Watson Ave, Suite 400
Beaverton, OR 97005

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

December 11, 2023

<<Notice of Data Breach>>

Dear <<FIRST NAME>> <<LAST NAME>>,

AvidXchange, Inc. (“AvidXchange”) provides payable automation software and payment solutions for middle market business and suppliers. We are writing to notify you of a recent incident that involved your personal information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it is appropriate to do so.

What Happened

In early April 2023, AvidXchange detected a cybersecurity incident as part of our routine security monitoring protocols. In response to the incident, we launched an investigation with the support of leading cybersecurity experts, reached out to law enforcement, expelled the unauthorized user from our systems, and accelerated our planned security enhancements. Our investigation revealed that the incident affected some of AvidXchange’s systems and that data from these systems was subject to unauthorized access or acquisition between March 2, 2023 and April 27, 2023. These data sets contained confidential information from our files, including personal information that was maintained as part of our regular business operations. We conducted a manual review of the personal information to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved

The following types of information related to you were extracted without authorization: name and <<Variable Text 1>>.

What We Are Doing

We have taken action to implement additional safeguards and harden our systems. These safeguards include: establishing separate, cloud-based user accounts to further limit and restrict the capabilities of privileged accounts; implementing additional logging processes and imposing more restrictions to limit access to sensitive systems; updating user access controls to require smart, context-dependent authentication; modifying firewall settings to further restrict inbound and outbound access to our environments; and deploying a new, highly secured virtual desktop environment. These safeguards are in place today, with many others being actively designed and implemented on an ongoing basis.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> 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 affected as part of this incident.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (888) 861-7014, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 29, 2024.

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 call (888) 861-7014 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

AvidXchange, Inc.

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or 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 (888) 861-7014 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. Credit report request should be staggered to 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. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: the District of Columbia Attorney General, 400 6th Street, NW, Washington, D.C. 20001; oag.dc.gov; Telephone: 1-202-727-3400.

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: 1-877-877-9392

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

PAUL HASTINGS

1(312) 499-6016
aaroncharfoos@paulhastings.com

December 9, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: Supplemental Notice of Security Event

To Whom it May Concern:

We represent AvidXchange, Inc. ("AvidXchange") located at 1210 AvidXchange Lane, Charlotte, North Carolina 28206. On October 13, 2023, we notified your office of a security event. We write to supplement that prior notice and notify you that the event also affected the security of certain personal information of approximately thirty-five (35) Maryland residents whose personal information AvidXchange was processing for Neighborhood Reinvestment Corporation d/b/a NeighborWorks America ("Customer"), one of AvidXchange's business customers. By providing this notice, AvidXchange does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data breach notification statute, or personal jurisdiction.

Nature of the Security Event

As we previously explained in our notice to your office on October 13, 2023, AvidXchange detected a cybersecurity incident as part of its routine security monitoring protocols on April 3, 2023. Upon learning of the incident, AvidXchange launched an investigation with the support of leading cybersecurity experts. Through its investigation, AvidXchange determined that the earliest evidence of unauthorized access was through a third party vendor. Ultimately, AvidXchange determined that certain systems were subject to unauthorized access or acquisition between March 2, 2023 and April 27, 2023. Additionally, AvidXchange determined that the incident affected some of AvidXchange's systems and that data from these systems was exfiltrated. Between May 2, 2023, and May 31, 2023, threat actors published several sets of data from the extraction. AvidXchange worked with a third party to review the data, which included internal, non-personally identifiable, corporate information. On September 27, 2023, AvidXchange confirmed that these data sets contained certain categories of personally identifiable information of employees, dependents, and investors. The categories of personally identifiable information include driver's license number, financial account number, credit card information, Social Security number, date of birth, electronic signature, health insurance information, and passport number.

Notice to Maryland Residents

AvidXchange provided notice to Customer of this event and offered to notify affected individuals. Customer has provided written notice of this event to affected individuals. This mailing includes notice to approximately thirty-five (35) Maryland residents impacted by the event who are affiliated with Customer.

VIA E-MAIL

Office of the Attorney General
December 9, 2023
Page 2

Other Steps Taken In Response

As we previously explained in our notice to your office on October 13, 2023, security is a critical concern and priority for AvidXchange, and the company has taken steps to implement additional safeguards and harden its system. These steps include:

- Expanding our threat detection capabilities and internal security protocol;
- Establishing separate, cloud-based user accounts to further limit and restrict the capabilities of privileged accounts;
- Modifying firewall settings to further restrict inbound and outbound access to our environments;
- Implementing additional logging and imposing restrictions to limit access to sensitive systems;
- Updating user access controls to require smart, context-dependent authentication; and
- Deploying a new, highly secured virtual desktop environment

Sincerely,

/s/ Aaron Charfoos

Aaron Charfoos
for PAUL HASTINGS LLP

Enclosure

EXHIBIT A



P.O. Box 989728
West Sacramento, CA 95798-9728

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

[DATE]

<<Notice of Data Breach>>

Dear <<FIRST NAME>> <<LAST NAME>>,

AvidXchange, Inc. ("AvidXchange") provides payable automation software and payment solutions for middle market business and suppliers, including <<DATA OWNER>>. We are writing on behalf of <<DATA OWNER>> to notify you of a recent incident that involved your personal information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it is appropriate to do so.

What Happened

In early April 2023, AvidXchange detected a cybersecurity incident as part of our routine security monitoring protocols. In response to the incident, we launched an investigation with the support of leading cybersecurity experts, reached out to law enforcement, expelled the unauthorized user from our systems, and accelerated our planned security enhancements. Our investigation revealed that the incident affected some of AvidXchange's systems and that data from these systems was subject to unauthorized access or acquisition between March 2, 2023 and April 27, 2023. These data sets contained confidential information from our files, including personal information that was maintained on behalf of NeighborWorks America, as part of our regular business operations. We conducted a manual review of the personal information to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved

The following types of information related to you were extracted without authorization: name and <<Variable Text 1>>.

What We Are Doing

We are protecting your information, as well as customer information, by taking action to implement additional safeguards and harden our systems. These safeguards include: establishing separate, cloud-based user accounts to further limit and restrict the capabilities of privileged accounts; implementing additional logging processes and imposing more restrictions to limit access to sensitive systems; updating user access controls to require smart, context-dependent authentication; modifying firewall settings to further restrict inbound and outbound access to our environments; and deploying a new, highly secured virtual desktop environment. These safeguards are in place today, with many others being actively designed and implemented on an ongoing basis.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> 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 affected as part of this incident.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (888) 861-7014, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is January 13, 2024.

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 call (888) 861-7014 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

AvidXchange, Inc.

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or 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 (888) 861-7014 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. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: the District of Columbia Attorney General, 400 6th Street, NW, Washington, D.C. 20001; oag.dc.gov; Telephone: 1-202-727-3400.

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: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. There are approximately [#] Rhode Island residents that may be impacted by this event.

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