15722

[IPP Letterhead]

[Insert Date]

[Name of Recipient]
[Street Address]
[City/State/Zip]

Dear [Name of Recipient]:

Independent Pet Partners Holdings LLC ("IPP") values its employees and is committed to protecting your personal information. Unfortunately, we are writing to inform you of an information security incident that could potentially affect you and to share with you the steps that IPP is taking to address it.

We recently discovered that a hacker placed malware onto a company device. This malware may have enabled the hacker to acquire documents received or sent from this device. Although the investigation did not uncover any indication that the hacker actually acquired company documents, the investigation also could not rule out this possibility.

Upon discovering the compromise, IPP promptly shut out the hacker and began reviewing all the documents transmitted to and from the device. On July 18, 2019, IPP discovered that one document contained personal information. Further careful review revealed that some of the other documents also contained personal information. We are writing you because your personal information was contained in the potentially compromised documents. This personal information included [mailing center to insert personal information via mail merge from spreadsheet].

**Please note that we have no information indicating that your personal information has been misused.**

Nevertheless, out of an abundance of caution, IPP is offering you eighteen months of identity protection services at no cost to you through IDShield. Your membership in IDShield provides identity restoration services, dark web monitoring, identity threat alerts, identity theft insurance, credit monitoring, which includes monitoring your credit file at all three national credit bureaus, and other benefits. To take advantage of this benefit, you must activate your IDShield membership before **September 30, 2019**. To activate your IDShield membership:

- **Visit** benefits.legalshield.com/ippcd, then click "Enroll Now", and on the next page click "Signing Up".
- **Enter** your state and click "Select Your Identity Theft Plan". Add the plan to your cart and input the requested contact information. Once you have completed this process, you will be asked to "Complete Purchase." Your screen will show a monthly total. You will not be responsible for the monthly total shown. Additionally, you will not be asked for a payment to enroll.

Once you have enrolled, you will receive a letter in the mail with your membership number.

We have included with this letter additional information on steps you can take to protect the security of your personal information. We urge you to review this information carefully.

IPP takes seriously both the security of your personal information and this incident. We have reported the incident to law enforcement and will cooperate with any investigation. We also have taken steps to prevent a recurrence, and we are conducting a thorough review of our security policies and procedures.

IPP sincerely apologizes for this incident and regrets any inconvenience it may cause you. Should you have questions or concerns regarding this incident, please do not hesitate to contact (877) 770-4903.

Sincerely,

Jeff David
Chief Executive Officer

## Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

**1. Enroll in IDShield.** You must personally activate identity monitoring for it to be effective. The notice letter contains instructions and information on how to activate your IDShield membership. If you need assistance, you should contact IDShield directly at 888-807-0407. IDShield will provide services including the following:

- **Credit Monitoring**: Actively monitors your Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration**: If you experience identity theft, a Licensed Private Investigator will assist you to restore your identity to its pre-theft status.
- **24/7 Emergency Assistance:** In the event of an identity theft emergency, IDShield provides emergency access to live support, ensuring you can get help right away.
- **Comprehensive Dark Web Internet Monitoring:** IDShield's comprehensive dark web internet monitoring provides extensive monitoring of the participant's personally identifiable information using intelligent analytics across the dark web, which is a series of black market websites where criminals purchase personal information.
- **Username/Password (Credentials) Monitoring:** IDShield monitors the internet for instances in which a member's username and password credentials have been exposed and alerts the member, enabling members to change their login information on any accounts that use the exposed credentials.
- **Social Media Monitoring:** IDShield monitors social media accounts to see if personal information has been exposed through images, captions, posts and comments.
- **Public Records Monitoring:** IDShield monitors over 78 billion public record reports from more than 10,000 diverse sources to screen for 34 different types of information, including name, address, phone number, email, and social security number.
- **$1 Million Identity Theft Insurance**[1]: Provides coverage for certain costs as a result of stolen identity.

Please direct questions about the IDShield product to its customer support team. A credit card is not required for enrollment in IDShield. Enrollment in IDShield will not affect your credit score. You are also eligible to use the IDShield Mobile App to access your identity protection services. The Terms and Conditions for this offer are located at https://idshield.cloud/terms-and-conditions.

**2. Review your credit reports.** You can receive free credit reports by placing a fraud alert. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three national credit bureaus. 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 from one of the three credit bureaus every four months.

**3. Review your account statements.** You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other service providers.

---

[1] Identity theft insurance is underwritten by a third-party insurance carrier. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

**4. Remain vigilant and respond to suspicious activity.** If you receive an e-mail or mail alert from IDShield and you have activated your IDShield membership, contact an IDShield private investigator. You should consider changing your username, passwords, security questions, and security answers to your online accounts. If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You also should consider reporting such activity to IPP, your local police department, your state's attorney general, and the Federal Trade Commission.

**5. You have the right to place a "security freeze" on your credit report at no charge.** A security freeze will prohibit a consumer reporting agency from releasing information in your credit file without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

To place a security freeze on your credit file, contact the three nationwide credit bureaus, listed below. You will need to provide appropriate proof of your identity to the credit bureau, which will include your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

The contact information for all three credit bureaus is as follows:

| Equifax | Experian | TransUnion |
|---|---|---|
| P.O. Box 105788 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19016 |
| 1-800-349-9960 | 1-888-397-3742 | 1-800-680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com |

**6. Consider placing a fraud alert with one of the three nationwide credit bureaus.** You can place an initial fraud alert by contacting one of the three nationwide credit bureaus listed above. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

An initial fraud alert stays in your file for at least one year. To place this alert, a credit bureau will require you to provide appropriate proof of your identity, which may include your Social Security number. If you are the victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years.

**7. You have the right to free copies of the information in your file (your "file disclosure").** An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide credit bureaus listed above. These additional disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change in your address.

**8. Additional Information.** You may obtain information about fraud alerts and security freezes and additional information about steps you can take to avoid identity theft from the following:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.ftc.gov/idtheft/
(877) IDTHEFT (438-4338)

**9. Police Incident Report.** Massachusetts law gives you right to report this incident to the police in the county where you reside and to receive a police incident report within 24 hours of filing.