EXHIBIT 1

By providing this notice, Print EZ does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data event notification statute, or personal jurisdiction.

Nature of the Data Event

During a routine review, Print EZ identified an anomaly in scan results for its e-commerce website printez.com. Upon receiving these results, Print EZ immediately commenced an investigation and later identified a suspicious file that was inserted into its e-commerce website. Print EZ quickly removed the infected file and took additional steps to secure its website. Additionally, Print EZ completely modified its checkout process to implement additional security measures. Print EZ determined on December 14, 2018 that it was unable to determine how the file may have affected information entered onto its website. In an abundance of caution, Print EZ is notifying customers who used a credit card on its website from September 1, 2016 until September 23, 2018 when Print EZ moved to its new checkout process.

The information that is collected on Print EZ's checkout page includes name, address, credit card number, expiration date, and CVV.

Notice to California Residents

After switching credit card processors in September 2018, Print EZ lost access to the billing address information for customers who made purchased from September 1, 2016 and September 23, 2018. Without this information, Print EZ was unable to provide written notice. On or about February 15, 2019, Print EZ provided notice to customers who made purchases between September 1, 2016 and September 23, 2018, which may include an unknown number California residents. Notice was provided by notifying state wide media in substantially the same form as the press release attached here as ***Exhibit A***. In addition, Print EZ is posted a copy of the notice on its website. A copy of the web posting is attached hereto as ***Exhibit B***.

Other Steps Taken and To Be Taken

Print EZ has security measures, polices, and procedures in place to protect data in its care and the company continues to review these measures as part of its ongoing commitment to the security of the information in our care. Print EZ implemented additional security measures to protect the payment card information entered into our website. Print EZ is also providing customers with information about this event and about steps individuals can take to better protect against misuse of personal information. Print EZ is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Print EZ is also providing written notice of this incident to other state regulators and the consumer reporting agencies, as necessary.

EXHIBIT A

PRINT EZ PROVIDES NOTICE OF DATA BREACH

FEBRUARY 15, 2019 (Monroe, New York) - Print EZ is taking steps to notify customers of a recent event that could potentially affect the security of some of its customer's payment card information. Print EZ take this incident seriously and is providing customers with information concerning this event in the abundance of caution. Print EZ also providing our customers with information and resources that can be used to better protect against the possible misuse of information.
on.

What Happened? During a routine review, Print EZ identified an anomaly in scan results for its e-commerce website printez.com. Upon receiving these results, Print EZ immediately commenced an investigation and later identified suspicious file that was inserted into its e-commerce website. Print EZ quickly removed the infected file and took additional steps to secure its website. Additionally, Print EZ completely modified its checkout process to implement additional security measures. Print EZ determined on December 14, 2018 that it was unable to determine how the file may have affected information entered onto its website. In an abundance of caution, Print EZ is notifying customers who used a credit card on its website from September 1, 2016 until September 23, 2018 when Print EZ moved to its new checkout process.

What Information Was Involved? The information that is collected on PrintEZ's checkout page includes the customer name, card number, card expiration date and CVV number.

What Print EZ Is Doing. Print EZ has security measures, polices, and procedures in place to protect data in our care and we continue to review these measures as part of our ongoing commitment to the security of the information in our care. Print EZ implemented additional security measures to protect the payment card information entered into our website. Print EZ is also providing customers with information about this event and about steps individuals can take to better protect against misuse of personal information.

What You Can Do. Print EZ encourages customers to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious activity. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report.

Customers have the right to place a "security freeze" on their credit report, which will prohibit a consumer reporting agency from releasing information in a credit report without express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in a person's name without consent. However, customers should be aware that using a security freeze to take control over who gets access to the personal and financial information in a credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application an individual makes regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, an individual cannot be charged to place or lift a security freeze on your credit report. Should a customer wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, customers will need to provide the following information:

1. Customer's full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;

4. If customer has moved in the past five (5) years, provide the addresses where the customer have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, an individual has the right to place an initial or extended "fraud alert" on a file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If an individual is a victim of identity theft, he/she is entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert on your credit file, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Customers can further educate themselves regarding identity theft, fraud alerts, security freezes, and the steps an individual can take to protect his/her personal information, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Customers can obtain further information on how to file such a complaint by way of the contact information listed above. Customers have the right to file a police report in the event of any actual or suspected identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, a person will likely need to provide some proof that he/she has been a victim. Instances of known or suspected identity theft should also be reported to other applicable law enforcement agencies and the state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, customers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 their file is limited; customers must give their consent for credit reports to be provided to employers; customers may limit "prescreened" offers of credit and insurance they get based on information in their credit report; and they may seek damages from violators. Customers 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. We encourage customers to review their 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.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, customers have the right to obtain any police report filed in regard to this incident. There are an unknown number of Rhode Island residents impacted by this incident.

For More Information. For individuals who may have further questions about this incident, please call our dedicated assistance line at 1 -845-782-2421. Additional information may also be found at www.printez.com.

EXHIBIT B

NOTICE OF DATA BREACH

FEBRUARY 15, 2019

Print EZ is taking steps to notify customers of a recent event that could potentially affect the security of some of its customer's payment card information. Print EZ takes this incident seriously and is providing customers with information concerning this event in the abundance of caution. We are also providing our customers with information and resources that can be used to better protect against the possible misuse of information.

What Happened? During a routine review, Print EZ identified an anomaly in scan results for its e-commerce website printez.com. Upon receiving these results, Print EZ immediately commenced an investigation and later identified suspicious file that was inserted into its e-commerce website. Print EZ quickly removed the infected file and took additional steps to secure its website. Additionally, Print EZ completely modified its checkout process to implement additional security measures. Print EZ determined on December 14, 2018 that it was unable to determine how the file may have affected information entered onto its website. In an abundance of caution, Print EZ is notifying customers who used a credit card on its website from September 1, 2016 until September 23, 2018 when Print EZ moved to its new checkout process.

What Information Was Involved? The information that is collected on Print EZ's check out page is the customer name, card number, card expiration date and CVV number.

What We Are Doing. Print EZ has security measures, polices, and procedures in place to protect data in our care and we continue to review these measures as part of our ongoing commitment to the security of the information in our care. Print EZ implemented additional security measures to protect the payment card information entered into our website. Print EZ is also providing customers with information about this event and about steps individuals can take to better protect against misuse of personal information.

What You Can Do. Print EZ encourages customers to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious activity. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report.

Customers have the right to place a "security freeze" on their credit report, which will prohibit a consumer reporting agency from releasing information in a credit report without express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in a person's name without consent. However, customers should be aware that using a security freeze to take control over who gets access to the personal and financial information in a credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application an individual makes regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, an individual cannot be charged to place or lift a security freeze on your credit report. Should a customer wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111

www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, customers will need to provide the following information:

1. Customer's full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If customer has moved in the past five (5) years, provide the addresses where the customer have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, an individual has the right to place an initial or extended "fraud alert" on a file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If an individual is a victim of identity theft, he/she is entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert on your credit file, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Customers can further educate themselves regarding identity theft, fraud alerts, security freezes, and the steps an individual can take to protect his/her personal information, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Customers can obtain further information on how to file such a complaint by way of the contact information listed above. Customers have the right to file a police report in the event of any actual or suspected identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, a person will likely need to provide some proof that he/she has been a victim. Instances of known or suspected identity theft should also be reported to other applicable law enforcement agencies and the state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, customers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 their file is limited; customers must give their consent for credit reports to be provided to employers; customers may limit "prescreened" offers of credit and insurance they get based on information in their credit report; and they may seek damages from violators. Customers 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. We encourage customers to review their 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.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, customers have the right to obtain any police report filed in regard to this incident. There are an unknown number of Rhode Island residents impacted by this incident.

For More Information. For individuals who may have further questions about this incident, please call our dedicated assistance line at 1 -845-782-2421.