Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, Pennsylvania 19103
aweaver@constangy.com
Direct: 941.875.5335

October 4, 2024

ONLINE SUBMISSION
Attorney General Bob Ferguson
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
Email: SecurityBreach@atg.wa.gov

RE: NOTICE OF DATA SECURITY INCIDENT

Attorney General Ferguson:

Constangy, Brooks, Smith & Prophete, LLP, represents 5.11, Inc. ("5.11") in connection with a recent data security incident described in greater detail below. 5.11 takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent on behalf of 5.11 because personal information for Washington residents may have been involved in the incident.

I. NATURE OF THE SECURITY INCIDENT

On August 5, 2024, 5.11 was alerted of unusual activity involving our online store. Upon discovering this activity, 5.11 took immediate steps to further secure its website and customer information. 5.11 also engaged a nationally-recognized digital forensics firm to conduct an independent investigation into the activity and determine whether any customer payment card information had been accessed or acquired without authorization.

After a thorough forensic investigation, on September 12, 2024, 5.11 determined that this incident may have involved payment card information for customers who purchased products through 5.11's online store between July 12, 2024 and August 22, 2024. 5.11 thereafter worked diligently to identify all potentially affected customers and provide them with appropriate notification.

II. NUMBER OF WASHINGTON RESIDENTS INVOLVED

On September 27, 2024, 5.11 determined that the notification population included 699 Washington residents. On October 4, 2024, 5.11 provided notification by first-class U.S. mail to these individuals via the attached notification letter template or a substantially similar version thereof.

The potentially affected personal information included names, email addresses, payment card numbers, expiration dates, and security codes.

III. Steps Taken to Address the Incident

As soon as 5.11 became aware of the incident, it took steps to further secure its website and conducted a comprehensive investigation. 5.11 also worked with the payment card brands and law enforcement to provide information related to the incident and has implemented additional measures to further enhance the security of its e-commerce platform and reduce the likelihood of a similar incident reoccurring.

5.11 has established a toll-free call center through IDX to answer questions about the incident and address related concerns. 5.11 has also arranged to provide all potentially affected customers with complimentary restoration assistance through IDX, which will work with individuals to help resolve issues with unrecognized payment card transactions.

IV. Contact Information

5.11 remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at aweaver@constangy.com.

Sincerely,

Aubrey Weaver
Partner
Constangy, Brooks, Smith & Prophete, LLP

Encl. Sample Notification Letter

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

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

October 3, 2024

Subject: Notice of <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>:

5.11 is writing to notify you of a data security incident relating to your purchase through our online store, 511tactical.com, which may have involved your payment card information. At 5.11, we take the privacy and security of your information very seriously so we are writing to inform you of the incident and the steps we have already taken, as well as to advise you about steps you can take to protect your information.

What Happened? In August 2024, 5.11 was alerted of unusual activity involving our online store. Upon discovering this activity, we took immediate steps to further secure our website and customer information. We also engaged a nationally-recognized digital forensics firm to conduct an independent investigation into the activity and determine whether any customer payment card information had been accessed or acquired without authorization.

What Information Was Involved? After a thorough forensic investigation, on September 12, 2024, we determined that this incident may have involved payment card information of customers who purchased products through our online store between July 12, 2024 and August 22, 2024. We then worked diligently to identify all potentially affected customers. The information that may have been involved includes names, email addresses, payment card numbers, expiration dates, and security codes.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. In addition, we reported the matter to the payment card brands and law enforcement in an effort to protect your information and prevent fraudulent activity. In order to reduce the likelihood of a similar incident occurring in the future, we have implemented additional measures to enhance the security of our e-commerce platform.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

In addition, 5.11 has arranged to provide its customers complimentary restoration assistance through IDX, a data breach and recovery services expert. If you identify any payment card transactions that you do not understand or that look suspicious, or if you suspect that any fraudulent transactions have taken place, you can contact IDX's Certified Recovery Advocates at 1-877-225-2109, who will work on your behalf to help resolve these issues. IDX's Certified Recovery Advocates are available Monday through Friday from 6:00 am and 6:00 pm Pacific Time.

For More Information. If you have any questions regarding this letter, we encourage you to contact our dedicated call center at 1-877-225-2109 between 6:00 am and 6:00 pm Pacific Time.

Rest assured, we take our customers' trust in 5.11, and this matter, very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Deborah Ajeska, Chief Administrative Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

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

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

October 3, 2024

Subject: Notice of <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>:

5.11 is writing to notify you of a data security incident relating to your purchase through our online store, 511tactical.com, which may have involved your payment card information. At 5.11, we take the privacy and security of your information very seriously so we are writing to inform you of the incident and the steps we have already taken, as well as to advise you about steps you can take to protect your information.

What Happened? In August 2024, 5.11 was alerted of unusual activity involving our online store. Upon discovering this activity, we took immediate steps to further secure our website and customer information. We also engaged a nationally-recognized digital forensics firm to conduct an independent investigation into the activity and determine whether any customer payment card information had been accessed or acquired without authorization.

What Information Was Involved? After a thorough forensic investigation, on September 12, 2024, we determined that this incident may have involved payment card information of customers who purchased products through our online store between July 12, 2024 and August 22, 2024. We then worked diligently to identify all potentially affected customers. The information that may have been involved includes names, email addresses, payment card numbers, expiration dates, and security codes.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. In addition, we reported the matter to the payment card brands and law enforcement in an effort to protect your information and prevent fraudulent activity. In order to reduce the likelihood of a similar incident occurring in the future, we have implemented additional measures to enhance the security of our e-commerce platform.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

In addition, 5.11 has arranged to provide its customers complimentary restoration assistance through IDX, a data breach and recovery services expert. If you identify any payment card transactions that you do not understand or that look suspicious, or if you suspect that any fraudulent transactions have taken place, you can contact IDX's Certified Recovery Advocates at 1-877-225-2109, who will work on your behalf to help resolve these issues. IDX's Certified Recovery Advocates are available Monday through Friday from 6:00 am and 6:00 pm Pacific Time.

For More Information. If you have any questions regarding this letter, we encourage you to contact our dedicated call center at 1-877-225-2109 between 6:00 am and 6:00 pm Pacific Time.

Rest assured, we take our customers' trust in 5.11, and this matter, very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Deborah Ajeska, Chief Administrative Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.