WILLIAM J. ROBERTS
Attorney at Law

Goodwin Square
225 Asylum Street
Hartford, Connecticut 06103
T: (860) 275-0184 F: (860) 881-2431
wroberts@daypitney.com

Via Online Data Breach Report Submission Form

July 27, 2026

Washington State
Office of the Attorney General
1125 Washington St. SE
PO Box 40100
Olympia, WA 98504

RE: Notification of Security Incident

Dear Office of the Washington Attorney General Representative:

On behalf of our client, SPay, Inc., a Delaware corporation d/b/a Stack Sports ("Stack Sports"), we are providing this notice to the Office of the Washington Attorney General of a security incident affecting approximately 1,190 Washington residents.

On June 8, 2026, Stack Sports identified suspicious activity affecting its SportsAffinity web application platform ("SportsAffinity Platform"), an online registration and payment platform used by athletic organizations and associations to facilitate athlete registration, program enrollment, and related payment processing, through its internal security monitoring mechanisms. Upon discovering the issue, Stack Sports immediately took steps to contain, investigate and remediate the activity, engaging an independent incident response team to assist with a forensic investigation and experienced cybersecurity counsel to advise on its response.

Stack Sports engaged nationally recognized experts to conduct a forensic investigation into the security incident, including determining the nature and scope of the unauthorized activity, identifying the information that may have been affected, and assessing the period during which the unauthorized activity was present. The investigation ended on July 8, 2026. On June 22, 2026, based on the initial findings of the investigation, Stack Sports was able to determine that the unauthorized activity began on or about May 8, 2026 and resulted from an unauthorized third party placing malicious code on the SportsAffinity Platform, which was then executed in users' web browsers when users accessed a payment checkout process. In addition, Stack Sports determined, based on the findings of the investigation, that the malicious code was fully removed from its servers by June 10, 2026 and that residual elements of the capture code remained in a limited number of customer browser caches until Stack Sports forcibly cleared it on June 22, 2026.

The investigation determined that the security incident was strictly limited to users of the SportsAffinity Platform who accessed the platform's checkout process during the incident window. The security incident did not involve other SportsAffinity users who did not access the platform's checkout process during the incident window or any of the company's Sports Connect Club platforms or any other Stack Sports platforms. The security incident also did not involve any data stored on the SportsAffinity Platform. The unauthorized actor did not remove any payment information stored on the SportsAffinity Platform as the SportsAffinity Platform does not store any payment information other than an encrypted transaction token.

Furthermore, based on the findings of the investigation, Stack Sports was able to determine that the security incident involved only payment information entered within limited online payment pages during the relevant period. The information potentially affected may have included: (1) cardholder name; (2) payment card number; (3) card expiration date; (4) card security code (CVV); and (5) checking account number (for those persons who may have paid by eCheck or ACH). The security incident did not involve consumers' Stack Sports account credentials, account profile information, or any documents that consumers may have uploaded or stored within their account. Furthermore, the investigation confirmed that no Social Security numbers or driver's license numbers were involved.

Relying upon the findings of the investigation, Stack Sports utilized its internal registration and payment records to identify affected residents. Stack Sports completed its identification of affected residents on July 17, 2026. This process included identifying customers, obtaining mailing addresses, ensuring de-duplication, and conducting a quality review of the final mailing list.

Stack Sports is notifying all affected individuals by first-class U.S. mail on July 27, 2026. A template copy of the notification being sent to Stack Sports consumers who were affected by this security incident is attached.

Stack Sports is offering all affected individuals complimentary identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include all of the following: twenty-four (24) months of CyberScan® monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

DAY PITNEY LLP

As a result of this security incident, Stack Sports has implemented additional security measures and enhanced monitoring protocols designed to detect and prevent similar activity moving forward, including the identification of opportunities to strengthen file-integrity monitoring and client-side script controls.

Please be assured that Stack Sports takes its obligation to protect the privacy and confidentiality of its consumers' personal information very seriously. If you have any questions, please contact me by phone at (860) 275-0184 or by email at wroberts@daypitney.com.

Sincerely,

William J. Roberts

William J. Roberts
Attorney at Law
Day Pitney LLP

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

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME
Or Visit:
https://response.idx.us/StackSports

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

July 27, 2026

RE: Notice of Security Incident

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

We are writing to let you know about a cybersecurity incident involving SPay, Inc. d/b/a Stack Sports ("Stack Sports," "we," "us") that may have involved certain payment card information you entered on our Sports Affinity web application platform (the "Platform").

This letter explains what happened, the information involved, the steps we have taken in response, and measures you can take to help protect your information.

1. What Happened

On June 8, 2026, Stack Sports identified suspicious activity affecting the Platform through its internal security monitoring mechanisms. We immediately took steps to contain, investigate and remediate the activity, engaging an independent incident response team to assist with a forensic investigation and experienced cybersecurity counsel to advise on our response.

On June 22, 2026, based on our review of the system, related data, and detection records, Stack Sports was able to determine the following timeline and details:

- **Incident Window:** The unauthorized activity began on or about May 8, 2026.
- **The Cause:** Unauthorized code was placed on the Platform by an unauthorized person. This code enabled the capture of certain payment-related information entered on a consumer's computers during the Platform's checkout process.
- **Mitigation:** The malicious code was fully removed from our servers by June 10, 2026. Residual elements of the capture code remained in an isolated number of customer browser caches until we forcibly cleared it on June 22, 2026.
- **Impact Verification:** Our team conducted a thorough review of all impacted transactions to identify affected individuals and their mailing addresses, finalizing this review on July 17, 2026.

This security incident was strictly limited to users of the Sports Affinity Platform during the incident window who accessed the Platform's checkout process. The incident did not involve other Sports Affinity users who did not access the Platform's checkout process during the incident window or any Sports Connect Club or any other Stack Sports platforms. The incident also did not involve any data stored on the Sports Affinity Platform. The unauthorized actor did not remove any payment information stored on the Sports Affinity Platform as the Sports Affinity Platform does not store any payment information other than an encrypted transaction token. Although we do not believe that this incident constitutes a breach under certain applicable laws, we are providing this notice to you so that you will know about it and be able to take action to protect your personal information if necessary.

2. How We Responded

Immediately upon discovering the incident, Stack Sports took decisive action to protect our users:

- **System Security:** We removed the unauthorized code and secured the Platform.
- **Expert Forensic Review:** We worked closely with leading incident response professionals and cybersecurity counsel to fully understand the nature and scope of the incident.
- **Future Prevention:** We implemented additional security measures and enhanced monitoring protocols designed to detect and prevent similar activity moving forward.

3. Types of Information Involved

Based on our review we have been able to determine that the incident involved only payment card information entered within limited online payment pages during the relevant period. The information potentially affected may have included:

- Cardholder name
- Payment card number
- Card expiration date
- Card security code (CVV)
- Checking account number (for those persons who may have paid by eCheck or ACH)

What was NOT involved: The incident did *not* involve your Stack Sports account credentials, account profile information, or any documents you uploaded or stored within your account. Furthermore, the investigation confirmed that **no Social Security numbers or driver's license numbers** were involved.

4. Protection of your information

We are providing written notices to all individuals that we have identified as having information potentially affected by this incident. Included with this notice is a "Reference Guide," which provides useful information regarding how to protect your identity, including obtaining copies of your credit report and implementing credit freezes. We encourage you to review the Reference Guide closely.

In addition, we are offering you twenty-four (24) months of identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 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 compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-855-830-6490, going to https://response.idx.us/StackSports, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9am - 9pm Eastern Time. Please note the deadline to enroll is October 27, 2026. Your unique enrollment code is <<ENROLLMENT>>.

We also encourage you to review your payment card statements for unauthorized charges. If you identify any suspicious activity, contact your card issuer immediately.

5. For more information

Stack Sports takes its obligation to protect the privacy and confidentiality of its consumers' personal information very seriously. While we do not think that the incident rises to the level of a breach under certain applicable laws, we regret that this security incident occurred and that it may have involved you. If you have any questions, you may contact our security team by email at incident.response@stacksports.com, call 1-855-830-6490, or go to https://response.idx.us/StackSports.

Sincerely,

Michael Hammond
General Counsel, Stack Sports

Reference Guide

<u>Review Your Account Statements.</u> We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately. The payment card brands' policies provide that cardholders have zero liability for unauthorized charges that are reported in a timely manner. Please contact your card brand or issuing bank for more information about the policy that applies to you.

<u>Order A Free Credit Report.</u> You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

<u>Report Incidents.</u> If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.

File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and about fraud alerts and security freezes:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
www.ftc.gov/idtheft/

<u>Consider Placing a Fraud Alert on Your Credit File.</u> To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 2002 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. For more information on security freezes, you may contact the three nationwide consumer reporting agencies, or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com/personal/credit-report-services/
Experian	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze/center.html
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-888-909-8872	www.transunion.com/credit-freeze

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

Your full name with middle initial and generation (such as Jr., Sr., II, III)

Your Social Security number

Your date of birth

Addresses where you have lived over the past five years

A legible copy of a government-issued identification card (such as a state driver's license or military ID card)

Proof of your current residential address (such as a current utility bill or account statement)

Social Security Card, pay stub, or W2

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.

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You may contact the Iowa Attorney General at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also place a security freeze on your credit reports, free of charge. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

For North Carolina Residents.

You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to law enforcement and the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
www.doj.state.or.us