ENTERTAINMENT & SPORTS

NIL Implications for Student-Athletes: Protecting Your Finances & Digital Identity

HUB

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

NIL has given student-athletes unprecedented financial visibility and opportunity, and with that comes a new responsibility to protect what they've built. Just as athletes apply discipline to their training, the same mindset applies to safeguarding their finances and digital identity: knowing who has access to their money and building strong habits to protect their information online. This guide outlines the most common risks athletes face and offers practical steps to stay protected, financially secure and in control.

Financial fraud

As the financial visibility of athletes grows, so does their exposure to fraud. The number and value of fraudulent cases targeting athletes have steadily increased over the past decade. Because athletes often earn substantial income at a young age — and may lack financial oversight or experience — they can become prime targets for sophisticated schemes.

Fraudsters typically gain trust through personal connections, family networks or professional relationships, then exploit that trust for financial gain. Without strong controls and professional guidance, even small, repeated losses can quietly accumulate into significant financial damage.

Common fraud schemes targeting athletes:

- **Impersonation of financial professionals.** Individuals posing as financial advisors or accountants misappropriate funds for personal use, including luxury purchases or debt repayment.
- **Unauthorized investments.** Representatives or advisors exploit their access by making risky, undisclosed investments in ventures where they hold personal financial interests.
- **Misuse of cash or power of attorney.** Agents, family members or associates with account access withdraw or divert funds for personal enrichment.
- **Misappropriation of earnings.** Designees fail to distribute earnings properly, redirecting funds for personal purposes.
- **Unauthorized NIL use.** Representatives or acquaintances exploit an athlete's name, image or likeness for endorsement deals or loans without consent.
- **False or misleading financial advice.** Fraudulent advisors inflate returns, conceal losses or involve athletes in Ponzi schemes.
- **Undisclosed conflicts of interest.** Advisors recommend investments tied to commissions or personal gain without full disclosure.

How athletes can mitigate fraud risk

To safeguard financial well-being, athletes must take a proactive, businesslike approach to personal finance.

- **Hire reputable, vetted professionals.** Engage licensed and credentialed third-party vendors or advisors (e.g., CPAs, CFPs) who meet professional standards and fiduciary obligations.
- **Formalize relationships in writing.** Establish contracts outlining each representative's responsibilities, compensation and authority to act.
- **Conduct regular financial reviews.** Schedule periodic reviews of bank accounts, investments and tax filings to detect irregularities early.
- **Require transparency.** Mandate regular financial disclosures and performance updates from all advisors or managers.
- **Include audit rights.** Incorporate independent audit rights into contracts to ensure oversight and deter misconduct.

By implementing these measures, athletes can significantly reduce vulnerability to financial exploitation. Building a professional advisory team and maintaining financial literacy are the strongest defenses against fraud — protecting both assets and long-term peace of mind.

Cybersecurity

With their high profiles, financial potential, and public exposure, college athletes have become increasingly attractive targets for cybercriminals. From phishing scams and identity theft to social engineering and data breaches, digital threats can cause reputational, financial and personal harm. Developing strong cybersecurity habits is now as essential as training for peak performance.

Protecting your digital identity

Cybersecurity begins with awareness. Many attacks succeed because athletes underestimate how much personal data they share or how easily it can be exploited. They must prioritize safe online behavior and strong digital hygiene to reduce exposure. This includes:

Strong password practices

- **Unique passwords.** Use different passwords for each account. Change them regularly, especially after a potential breach.
- **Password managers.** Use reputable password management tools to create and store complex, unique passwords securely.
- **Multi-factor authentication (MFA).** Enable MFA wherever possible for an additional layer of security.

Social media awareness

- **Privacy settings.** Regularly review privacy settings to control who can view your posts, photos, and personal information.
- **Limit personal information.** Avoid sharing sensitive details such as addresses, financial information or travel plans. Engage a vetted social media management service if professional assistance is needed.
- **Phishing and scams.** Be cautious of suspicious links, QR codes or messages — especially those impersonating trusted sources. Always verify before clicking or responding.
- **Reputation management.** Remember that every post contributes to your personal brand. Avoid controversial or impulsive content that could harm your reputation or career.

Secure devices and networks

- **Regular updates.** Keep operating systems, apps and firmware current to close known security gaps.
- **Antivirus protection.** Use reputable antivirus software to detect and block malware or spyware.
- **Safe Wi-Fi practices.** Avoid public Wi-Fi for sensitive transactions. If necessary, connect through a virtual private network (VPN).
- **Device protection.** Lock screens when not in use and use biometric or PIN access controls.

Financial and personal data security

- **Monitoring accounts.** Regularly review bank, investment and credit card statements for unauthorized activity.
- **Securing transactions.** Use only encrypted sites ("https") and avoid online purchases or banking over public Wi-Fi.
- **Verifying financial advisors.** Work only with licensed and vetted professionals. Be wary of unsolicited offers or investment pitches.

Recognize and prevent social engineering

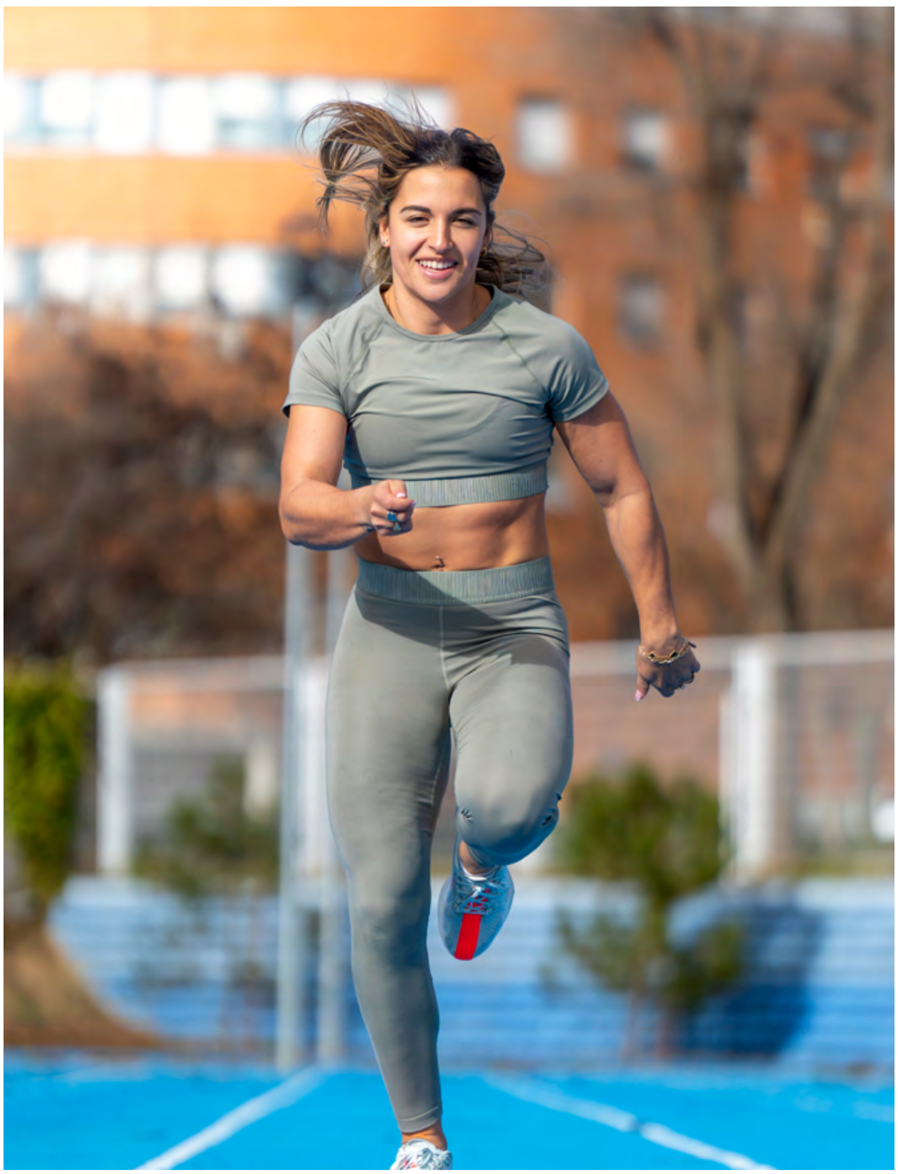
- **Pause before you click.** Cybercriminals rely on urgency and fear to elicit quick action. Take time to verify.
- **Confirm requests.** Validate any request for money, access or sensitive information directly with the source.
- **Report suspicious activity.** Alert your athletic department's IT team, advisor or local authorities if you suspect an attempted scam.

Building cyber resilience

Education is the cornerstone of prevention. Athletes should stay informed about emerging threats and evolving scams. They should approach online interactions with a healthy dose of skepticism.

Work with the right broker

Successfully navigating the NIL landscape requires partnering with advisors who understand the unique challenges student-athletes face. HUB's Entertainment and Sports team works with athletes and athletic departments nationwide, providing guidance on risk management, financial planning and long-term protection. Connect with HUB today to help you build a foundation for lasting success.



Strategic support that puts you in control.

When you partner with us, you're at the center of a vast network of experts who will help you reach your goals. With HUB, you have peace of mind that what matters most to you will be protected — through unrelenting advocacy and tailored solutions that put you in control.

For more information on Name, Image, and Likeness, contact a sports insurance specialist.

hubinternational.com/sports

Ready for tomorrow.

Risk & Insurance | Employee Benefits | Retirement & Private Wealth