PZENA Investment Management

Fraud and Phishing Awareness Notice

Protecting Our Clients, Partners, and Candidates from Fraudulent Activity

Important Notice

Pzena Investment Management, LLC (**"Pzena"**) has become aware of an increase in fraudulent schemes targeting investors, job seekers, vendors, and members of the public. In these schemes, bad actors may use our name, brand, executive names, and official-looking materials to impersonate Pzena in order to deceive individuals into transferring funds, divulging sensitive personal information, or accepting fictitious employment offers.

Pzena does not endorse or have any connection to these activities. This notice is issued to alert current and prospective clients, counterparties, job applicants, vendors, and the general public to these unlawful practices. We urge anyone who receives suspicious communications purportedly from Pzena to exercise caution and verify authenticity through our official channels before taking any action.

Official Communications Channels

Pzena communicates exclusively through the following official channels:

Website:	www.pzena.com
Email:	All official Pzena email addresses end in @pzena.com
Social Media:	LinkedIn (linkedin.com/company/pzena-investment-management) X (https://x.com/PzenaInvstmtMgt)
Phone:	Published contact numbers listed on www.pzena.com/contact

Any website, email domain, social media account, or telephone number that does not match the above should be treated with extreme caution. Pzena does not conduct business, solicit investments, or communicate with clients or candidates through personal email accounts (e.g., Gmail, Yahoo, Hotmail), encrypted messaging applications (e.g., WhatsApp, Telegram, Signal, WeChat), or unofficial social media profiles. We also do not offer, endorse, or otherwise promote Pzena-branded applications for commercial use.

Common Fraudulent Schemes

1. Impersonation and Brand Spoofing

Fraudsters may create fake websites, social media profiles, applications, and email addresses designed to closely resemble Pzena's official presence. They may use Pzena's logo, executive names, and marketing materials without authorization. These communications may appear highly convincing, including fake account statements, fabricated performance data, or counterfeit correspondence.

2. Fraudulent Investment Solicitations

Individuals may be contacted by parties falsely claiming to be Pzena representatives and offered unsolicited investment opportunities, including promises of guaranteed or unusually high returns, access to exclusive or restricted funds, or cryptocurrency-based investment schemes. Legitimate investment management firms, including Pzena, do not solicit investments through unsolicited outreach, social media messages, or messaging apps, and we do not guarantee investment returns.

3. Recruitment and Employment Scams

Scammers may pose as Pzena recruiters or hiring managers and contact job seekers through platforms such as LinkedIn, WhatsApp, or email. These fraudulent approaches may involve fake job postings, fabricated offer letters, or requests for personal information and advance payments under the guise of onboarding. Pzena will never request any form of payment as part of the hiring process, nor will we conduct interviews exclusively via text, messaging apps, or consumer-grade video platforms (e.g., Google Hangouts) without prior formal contact through official channels.

4. Phishing, Smishing, and Vishing

Phishing emails, text messages (smishing), and fraudulent phone calls (vishing) may purport to come from Pzena and ask you to verify account details, click on a malicious link, open an attachment, or call back a fraudulent number. These communications are designed to capture personal data or install malware on your device.

5. Wire Transfer and Account Fraud

Bad actors may impersonate Pzena clients, executives, or counterparties to request unauthorized fund transfers, changes to payment instructions, or access to account credentials. Any unexpected or unusual instruction involving the movement of funds should be treated as a potential fraud attempt and independently verified with your known Pzena contact.

What Pzena Will Never Do

As a matter of firm policy, Pzena will never

- Contact you unsolicited to solicit investments or request personal financial information.
- Request payment of any kind in connection with recruitment or onboarding.
- Ask you to transfer funds to a personal bank account, a third-party account, or via cryptocurrency.
- Offer guaranteed returns or risk-free investment opportunities.
- Request that you act immediately or under time pressure to complete a financial transaction.
- Conduct business or interviews exclusively through WhatsApp, Telegram, WeChat, or similar platforms.
- Request that you send sensitive personal information (e.g., Social Security number, passport, banking credentials) through unsecured or unverified channels.
- Ask for payment to release, unfreeze, or transfer existing investments.

PZENA Investment Management

Warning Signs of Fraud

Be alert to the following red flags:

- Email addresses that differ slightly from @pzena.com (e.g., @pzena-invest.com, @pzenainvestments.net, or free-provider domains)
- Websites that mimic the look and feel of www.pzena.com but use different domain names or URLs
- Unsolicited offers that promise unusually high returns or exclusive access to funds not publicly offered
- Requests for personal information or financial credentials early in an investment or recruitment process
- Communications that create urgency, pressure you to act quickly, or discourage you from seeking independent advice
- Grammar or spelling inconsistencies in communications claiming to be from Pzena
- Requests to communicate or transact exclusively through encrypted messaging apps or unofficial platforms
- Job offers made without a formal interview process conducted through official Pzena systems

If You Suspect Fraudulent Activity

If you believe you have received a communication that fraudulently uses Pzena's name or identity, or if you suspect you may have been targeted by a scam:

1. Do not respond, transfer funds, or provide any personal or financial information.
2. Preserve all records of suspicious communication, including emails, screenshots, phone numbers, and any documents received.
3. Contact Pzena directly using the verified contact information on our official website (www.pzena.com) to report the incident and confirm whether the communication is legitimate.
4. Report the incident to the relevant law enforcement authorities in your jurisdiction. In the United States, you may also file a report with the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov or the Federal Trade Commission (FTC) at reportfraud.ftc.gov.
5. If funds have been transferred, contact your financial institution immediately to attempt to halt or reverse the transaction.

Contact Us

To verify the legitimacy of any communication or to report suspected fraud, please contact us through our official website at www.pzena.com or reach out to Pzena's fraud awareness team via email at fraudmonitoring@pzena.com. Do not rely on contact information provided in a communication you believe may be fraudulent.