

Indiana MoneyWise

A publication provided by THE INDIANA SECRETARY OF STATE



Threats
facing investors

Protecting yourself in
the age of
identity theft

OLD DOGS NEW TRICKS

old fraud schemes repackaged with new methods

PLUS

Think you know how to spot fraud?
Test yourself!

Dear Hoosiers:

Thank you for reading the Indiana Secretary of State's e-magazine. The purpose of this publication is to provide Hoosiers with timely tips and information on smart money management skills and how to be financially fit.



Investment fraud has been around for ages. Scams like Ponzi schemes gained popularity in the 1920s. However, no matter how old the scheme, criminals will find new ways to put them in shiny packages to attract new victims. These packages can include new technology such as virtual currency or hot topics of the day like Ebola.

This e-magazine edition focuses on investment fraud schemes ranging from older schemes like pump and dump to newer scams such as marijuana stock schemes. Learn how to identify scams and how to protect yourself from investment fraudsters. Remember, being educated is the best weapon against investment fraud!

Sincerely,

A handwritten signature in black ink that reads "Connie Lawson". The signature is fluid and cursive, with the first name "Connie" being more prominent than the last name "Lawson".

Indiana Secretary of State

MISSION STATEMENT

It is the mission of the office of Secretary of State Connie Lawson to deliver to the people of Indiana government-as-a-service that focuses on unqualified integrity and accuracy in our elections, consistent and principled regulatory methods, ceaseless protection of Hoosier investors, and the most efficient use of taxpayer resources.

What services make up the Secretary of State's office?



There are four main divisions that comprise the Secretary of State's office:

Business Services
Securities

Elections
Auto Dealer Services

The Office of Secretary of State is one of five constitutional officers originally designated in Indiana's State Constitution of 1816. Sixty-one Hoosiers have served as the third highest-ranking official in state government.

Duties of the office include registering new business, regulation of the securities industry, oversight of state elections, commissioning of notaries public, registration of trademarks and licensing of vehicle dealerships throughout Indiana.

TOP NEW AND OLD THREATS

While new threats to investors pop up every year, the most popular scams have been around for ages. To help protect investors, the North American Securities Administrators Association or NASAA releases a list of the top threats facing investors and business owners. This e-magazine will focus on some of the emerging schemes and how old schemes are being repackaged. But first, let's go over NASAA's top threats.



THREATS FACING INVESTORS

EMERGING SCHEMES

Binary Options

* These are securities in the form of option contracts that have a payout dependent on whether an underlying asset increases or decreases in value.

Marijuana Investment Schemes

* Learn more about these in our story on page 10 of this magazine.

Stream-of-Income Investments

* Scammers get investors to invest in companies that produce monthly returns by selling a stream of income such as pension payments.

Virtual Currency

* Learn more about these in our story on page 13 of this magazine.

PERSISTENT THREATS

Ponzi Schemes

* The schemes promise unbelievably high rates of return. They gain momentum because initial investors are paid a substantial return in hopes they will spread the word and attract new investors.

Private Offerings

* An exemption in federal securities law allows private placements to be sold to investors without registration. Private offerings have little regulatory oversight and carry a high risk.

Real Estate Investment Schemes

* Schemes related to the development, purchase, renovation and flipping of distressed properties remain popular.

Affinity Fraud

* This type of fraud preys on the trust of members of a targeted group, organization or community by exploiting similarities of the members. Affinity fraudsters target religious and ethnic groups, the elderly, recent immigrants and business associates.

Oil and Gas Drilling Programs

* Oil and gas drilling investments are appealing alternatives for investors who are frustrated with stock market volatility or skeptical of Wall Street. They involve a high degree of risk, so they're only suitable for investors who can bear a substantial loss.

OLD DOGS NEW TRICKS

HOW TO SPOT OLD SCAMS USING NEW METHODS

Social media is a great way for us to connect with family, friends and colleagues. Facebook, LinkedIn and Twitter have changed the way we interact with each other and the way we gather information. One thing that hasn't changed is the existence of investment fraud. Social media gives scammers new avenues to pursue their victims. Instead of being confined to their community, scammers can now reach millions of potential victims. Even former con artist Frank Abagnale (the inspiration for the movie "Catch Me if You Can") admits technology makes committing fraud a lot easier than it used to be.

PROTECT YOURSELF

BY FOLLOWING THESE SIMPLE RULES

Never give out personal information on a social media website.

Don't respond to unsolicited emails.

Ensure websites are legitimate

Don't just accept anyone's friend request.

Update security information.





BE ON THE LOOKOUT

FOR OPPORTUNISTIC SCAMS

Scammers love to use headlines of natural disasters and contagious diseases as way to scare people into investing in phony scams. Below are just a few that have happened in recent years:

Ebola

Due to last year's Ebola outbreak in Western Africa and its presence in the United States, internet scams related to Ebola "stocks" and "investments" started to pop up. The NASAA found nearly 1,200 new domains with "Ebola" in their name just since April 2014.

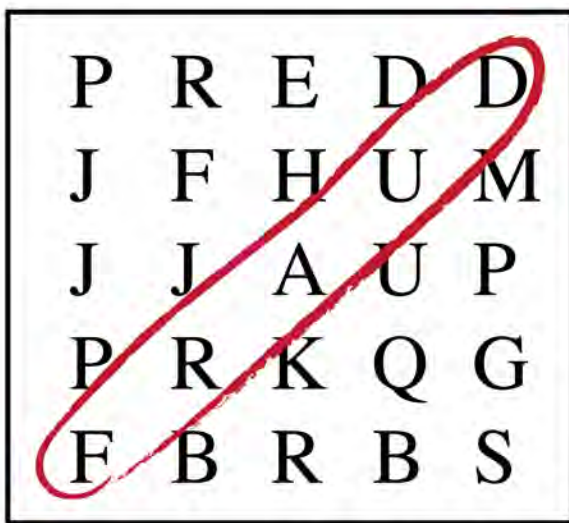
Hurricane Sandy

Investment and charity scams after Hurricane Sandy swelled due to social media. Americans wanted to help those who had lost everything and scammers used that vulnerability to prey on victims. These are typically ran through the internet so you can't judge their sincerity.

Terrorism

After September 11, 2001, Americans were on a higher level of alert. Scam artists use this vulnerability by crafting scams using defense-related companies, anti-terrorism or protection from biological or chemical attacks. Scammers use patriotic claims or that they are contracted with the federal government.

To avoid these scams, always do your research. Sometimes a quick Google search will bring up information on the validity of the scam. If not, check with the Indiana Secretary of State's Securities Division.



THINK YOU KNOW HOW TO SPOT FRAUD?

TEST YOURSELF!

Take this test from the North American Securities Administrators Association to see if you are prepared to protect yourself. Click [here](#) for the online version.

1. Which of the following phrases should raise your concern about an investment?
 - A. High rate of return
 - B. Risk-free
 - C. Your investment is guaranteed against loss
 - D. You must invest now
 - E. All of the above
2. Securities laws protect investors by requiring companies to:
 - A. Show profits before they can sell stock
 - B. Provide investors with specific information about the company
 - C. Pay dividends
 - D. Repay investors who have lost money
3. In which situation are you taking the least amount of risk?
 - A. Buying a Certificate of Deposit (CD), in the United States, or a Guaranteed Investment Certificate (GIC) in Canada, from a bank
 - B. Investing with someone you know through your church or community
 - C. Investing offshore
 - D. Investing with someone who contacted you by phone.
4. A fellow book club member tells you about an investment opportunity that has earned returns of 20% during the past year. Your investments have been performing poorly and you're interested in earning higher returns. This person is your friend and you trust them. What should you do?
 - A. Ask your friend for more information about the investment so that you can understand the risks before you make a decision
 - B. Invest only a small amount to see how things go before making a larger investment
 - C. Call your securities regulator to see if the investment has been registered or is properly exempted for sale
 - D. A and C
5. Which of the following should you rely upon when making an investment decision?
 - A. Testimonials of other investors
 - B. Advertisements and news stories in the media or on the Internet
 - C. Technical data that you don't really understand
 - D. Information filed with your securities regulator
6. Ways to protect yourself from investment fraud include:
 - A. Read all disclosure documents about an investment
 - B. Seek advice from an independent and objective source
 - C. Be skeptical and ask questions
 - D. Never write the check/cheque for an investment in the name of your salesperson
 - E. All of the above

7. When dealing with a securities salesperson who is considered reputable, you should do all the following except:

- A. Request copies of opening account documentation to verify that your investment goals and objectives are stated correctly
- B. Open and review all correspondence and account statements when you receive them
- C. Verify your written account statements with information you can obtain online
- D. Allow the salesperson to manage your assets as they see fit because they are the expert
- E. Evaluate your salesperson's recommendations by doing your own independent research

8. Which of the following are frequently used to defraud the public?

- A. Short-term promissory notes
- B. Prime bank investments
- C. Offshore investments to avoid taxes
- D. Nigerian advance fee letters
- E. All of the above

9. The role of government securities regulators is to:

- A. Sell shares to investors
- B. Act as an association for securities dealers and advisers
- C. Regulate securities markets, the investment industry and protect investors
- D. All of the above

10. You've worked closely with your securities advisor for years. Recently, he asked you to invest in a product that he is really excited about, however, the recommendation seems very different from financial products you've invested in previously. Which of the following should you do?

- A. Agree to make the investment because you have done business with your salesperson for years and trust them implicitly
- B. Check with your securities regulator to see if they have any information on the investment product
- C. Check with your securities regulator to see if the securities salesperson is authorized to sell the product in question
- D. Rely upon the written material the salesperson gives you
- E. A & D only
- F. B & C only

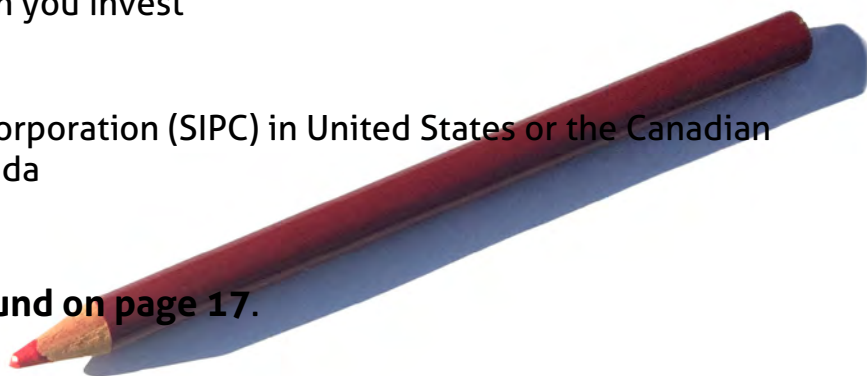
11. An investment is likely to be legitimate if:

- A. The promotional materials and company website look professional
- B. The company has a prestigious office location
- C. Other investors are receiving quick up-front returns
- D. The company has an official-sounding name
- E. None of the above

12. Who insures you against investment losses?

- A. No one; this is the risk you take when you invest
- B. My securities regulator
- C. The company selling the investment
- D. The Securities Investor Protection Corporation (SIPC) in United States or the Canadian Investor Protection Fund (CIPF) in Canada

Answers to the questions can be found on page 17.



MARIJUANA STOCK SCAMS:

Dont let your money go up in smoke

As states begin to legalize the use of marijuana, there has been an increase in marijuana-based investments or pot stocks. This creates new opportunities for scammers to convince victims to invest in fraudulent companies through traditional pump and dump schemes. In many cases, the scammers attract investors with false, but optimistic information on the potential of stock in thinly traded company with little to no financial success. When the stock hits a high point, the scammers then sell off all their shares and leave the remaining investors with stock that is worth nothing.

FINRA suggests ways to avoid potential scams:

- When approached by a stranger regarding an investment opportunity, ask why they would approach you.
- Be wary of companies with strong promotions and those that issue a lot of press releases within a small amount of time. This is typically a sign of “pumping” the price.
- Research, research, research. With every investment opportunity, you should do your due diligence and check out the product and the seller to make sure they are registered.
- Know where the stock trades, whether it is the NASDAQ or other registered national securities exchanges or an over-the-counter (OTC) platform like Over-the-Counter Bulletin Board. Stocks sold on OTC have minimum standard requirements and may not have the liquid market as stocks on national exchanges.
- Read a company’s SEC filings to verify information you have heard about the company.
- Watch out for companies that change their name or business focus frequently.

For more information on how to protect yourself from these types of scams, review the SEC’s Investor Alert on marijuana-related investments.

PUMP AND DUMP

An old scam with new angles

Pump and dump schemes are nothing new to the investment world. This is where investors are lured by flashy promotions and advertising as a way to create a demand for a company's stock. Once the share price is high, scammers quickly sell their shares, leaving them with a profit and legitimate investors with worthless stock.

Like the RCA and the "Radio Pool" scheme that came as popularity of the radio grew, new technology brings new opportunities to be scammed. Pump and dumpers today capitalize on popular markets as a way to lure investors into the next big thing. Typically red flags to pump and dump schemes are

- *Often confined to the internet
- *Aggressive promotions
- *Frequent name changes of companies to whatever the hot topic is of the moment
- *A barrage of press releases hyping the stock with optimistic information
- *Promotional materials on social media sites and emails

THE RED FLAGS OF FRAUD

Old or new, it is still important to know

Despite whether it is a traditional Ponzi scheme or a scam ran through social media, investment scams have common red flags. Knowing what those flags are will help keep you from becoming a victim.

Unsolicited emails or social media

- Don't respond to these without doing further research.

Guarantees

- As the saying goes, there are only two guarantees in life: death and taxes. Be skeptical about anyone who "guarantees" investments will provide high returns.

Unregistered products

- Most scams have to do with unregistered securities. Always check with your securities regulator to see if the product is registered.

Overly consistent returns

- Investments that only go up or stay consistent each month should raise suspicion. Stocks should fluctuate, especially in difficult economic times.

Complex strategies

- Scammers will give complex explanations to make sure you don't understand what you are getting into.

Missing documentation

- Always ask for written information about an investment. Lack of documentation may indicate an unregistered securities.

SENIOR MEDICARE PATROL



WORKING TO FIGHT FRAUD AND ABUSE

You've probably heard your friends and neighbors tales of Medicare fraud: scam artists asking for your Medicare card, providers charging for procedures you never had or charging Medicare patients higher rates.

Thankfully, in Indiana, there are senior citizens on patrol.

This isn't your typical neighborhood crime watch. Instead, it's a statewide network of volunteers charged with helping you avoid Medicare fraud and abuse. They are called the Senior Medicare Patrol (SMP) and they want to save you from Medicare and Medicaid scams.

Nationwide, it's estimated that Medicare and Medicaid fraud and abuse costs taxpayers \$60 billion a year, so the work SMP is doing not only helps seniors, but also taxpayers who eventually shoulder the burden of these expenses.

SMP staff and their highly trained volunteers conduct outreach to Medicare beneficiaries, caregivers and the professionals that serve them in their communities through group presentations, exhibiting at community events, answering calls to the SMP help lines and one-on-one counseling. Most SMP volunteers are retired Medicare beneficiaries and thus well-positioned to assist their peers.

Their primary goal is to teach beneficiaries how to protect their personal identity, identify and report errors in health care bills, and spot deceptive health care practices. If you suspect that you are a victim of fraud, reach out to your local Area Agency on Aging by calling 800.986.3505. The SMP volunteers in your area will help you take action to prevent, detect or report Medicare fraud and abuse.

Additionally, the Senior Medicare Patrol is always looking for more volunteers. You can join the Patrol by contacting the Area Agency on Aging or calling the SMP office directly at 317.205.9201.

For more information or to report potential Medicare fraud or abuse contact: 1.800.986.3505 or <http://www.iaaaa.org/smp.asp> or www.facebook.com/INSMP.





VIRTUAL CURRENCY





MONEY OF THE FUTURE OR HIGH TECH SCAM?

So what is virtual currency anyway? Virtual currency is an electronic medium of exchange that can be bought or sold through virtual currency exchanges and used to purchase goods or services where accepted. These currencies are stored in an electronic wallet, also known as an e-Wallet, which is a digital system allowing payments online.

Virtual currency, which includes digital and crypto-currency, are gaining in both popularity and controversy. Growing numbers of merchants, businesses and other organizations currently accept Bitcoin, one example of crypto-currency, in lieu of traditional currency. The U.S. Federal Election Committee has authorized Bitcoin for donations to political action committees.

Recently, one of the largest Bitcoin exchanges, MtGox, shut down after claiming to be the victim of hackers and losing more than \$350 million of virtual currency. Despite the controversy, virtual currency may find its way into your e-Wallet.

Some common concerns investors should consider before investing in any offering containing virtual currency include:

-  Virtual currency is subject to minimal regulation, susceptible to cyber-attacks and there may be no recourse should the virtual currency disappear.
-  Virtual currency accounts are not insured by the Federal Deposit Insurance Corporation (FDIC), which insures bank deposits up to \$250,000.
-  Investors will be highly reliant upon unregulated companies lacking the internal controls, making them more susceptible to fraud and theft.
-  Investors will have to rely upon the strength of their own computer security systems, as well as security systems provided by third parties, to protect their e-Wallets from theft.

Protecting Yourself in the Age of Identity Theft

Identity theft is a reality we must deal with in our world today. I know from personal experience how scary, frustrating, and helpless having your identity stolen can feel. When my identity was stolen in 1998 I spent four months attempting to clear my name and re-take control of my identity. It was horrible. But here's the thing, it was absolutely my fault. I left my wallet and my checkbook in my car, where it was stolen and then used to open lines of credit in my name. It was completely avoidable. There are types of identity theft you can avoid by simply doing the following:

1) Don't carry your life on your person

Ladies, I'm talking about your purses. Gents, I'm talking about your wallets. You don't need to carry every form of identification with you at all times. Social Security cards need to be in a safe at home. There's no need to hand your identity over to thieves on a platter.

2) Be careful with email

Email "phishing" scams are one of the most common forms of identity theft. To be on the safe side don't click links in emails that appear to be from any of your service providers (banks, cell phone company, etc.). Advanced scams can create websites that look deceptively similar to your service provider. Just as a precaution, access your service provider's web address via typing the known website into a browser as opposed to clicking links from an email.

3) Shred everything

Everything.

4) Get creative with usernames and passwords

It's easy to get in a password rut when certain services require a password change every other day (or so it seems). But you've got to fight this. Get creative. Avoid the 'KidsName123' passwords and go for something with lots of #*\$#(%&. I'm not cursing at you, I really mean use lots of #)@\$U(@*. Will it be hard to remember? Sure. But will it help keep your information protected? Absolutely.

5) Check your credit report every year

It's easy to assume you know everything going on in your financial life, but a credit report will show you what's going on that you don't know about. Don't wait 5 years to check your report. You could find out that someone has been living the good life off of your name in Sedona. Check your credit report every year to monitor your financial life and to avoid any surprises.

Those are simple ways you can protect yourself every day, yet these tips will only protect you from certain types of identity theft. There are two primary types of security breaches: financial account breaches and identifying information breaches. When Target and Home Depot got hacked recently, financial accounts were stolen. This means that if you used a

Continued from previous page

you used a debit or credit card at those stores, then your card numbers were stolen. It's very frustrating when someone steals your account numbers, but the solution is quite simple. You file a fraud report for the charges that aren't yours, and then you get a replacement card with new numbers. I've been the victim of this type of theft no less than five times. It's an unfortunate reality of commerce in the 21st century.

On the other hand, identifying information breaches are a big deal for consumers. If someone were to steal your Social Security number, date of birth, address, and other private information, then the thief could open a new credit account in your name, anytime they want...forever. Your date of birth does not change. Your Social Security number does not change. You can't clear the problem by changing your numbers. Those particular numbers are unchangeable. The only, and I repeat, **ONLY** way to protect yourself is to prevent new credit lines from opening. The only way to do that is to freeze your credit.

Freezing your credit simply prevents others from accessing your credit for the purpose of opening new credit lines. If you were to freeze your credit today, go shopping, and then try to open a store credit card, then it would be declined immediately. While freezing your credit **DOES NOT** affect your current credit lines, it will affect someone's ability to run your credit score when you need to rent an apartment or buy a car. You should temporarily lift the credit freeze the week before you need your credit score run. Freezing your credit **DOES NOT** hurt your credit score.

Mercifully, freezing your credit is a painless process. Simply go to the websites of the three main credit bureaus (Equifax, Experian, and TransUnion) and follow the instructions to freeze your credit. In the state of Indiana it is free to freeze your credit. Each bureau will ask you to generate a PIN number, and it's extremely important you maintain this number. You will need this PIN to unfreeze your credit in the future.

I don't need to tell you how important your identity is. Take these few steps to protect yourself and in the event your identity is stolen, take action quickly. Protecting your identity is a big part of your financial life. Don't neglect to protect yourself.

Peter Dunn a.k.a. Pete the Planner® is an award-winning comedian and an award-winning financial mind. He's the author of ten books, six of which were featured in a nationwide launch at Barnes & Nobles stores in January of 2015. He is the host of the popular radio show [The Pete the Planner Show on 93 WIBC FM](#) and is a columnist for the Indy Star. Pete has appeared regularly on CNN Headline News, Fox News, Fox Business as well as numerous nationally syndicated radio programs. In 2012, Cision named Pete the fourth most influential financial broadcaster in the nation. For more information visit petetheplanner.com.



HOOSIER LOTTERY AND IVY TECH TEAM UP TO PROVIDE ONLINE FINANCIAL LITERACY

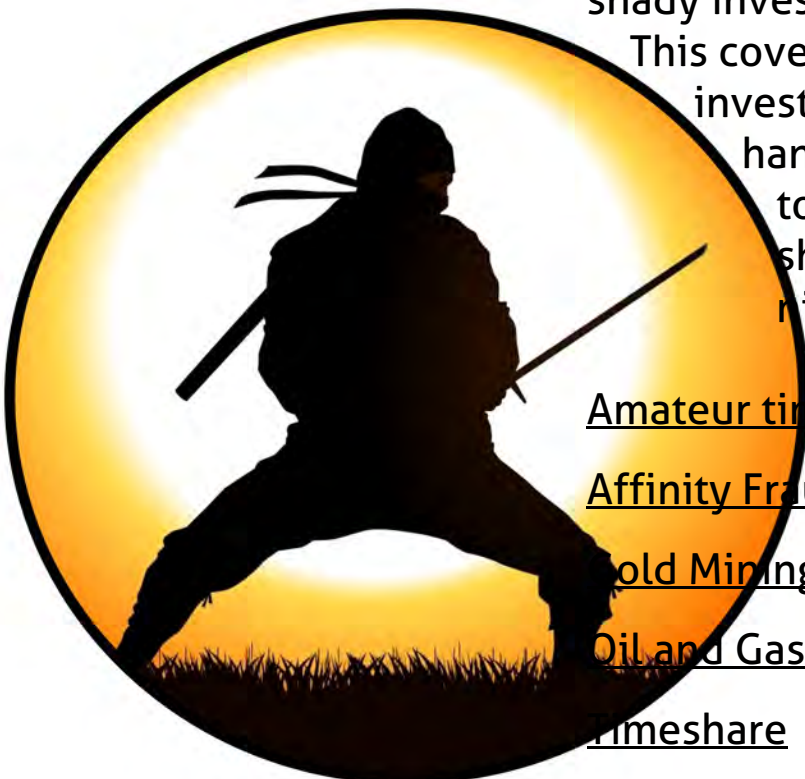


In February, the Hoosier Lottery and Ivy Tech Community College worked together to launch a Massive Open Online Course or MOOC. This interactive online course allows participants to learn how to manage credit, pay off debt, plan retirement and other general financial literacy topics. The course is free and available to all Hoosiers. For more information of the course, visit www.learnfinancialliteracy.com.

FRAUD NINJA

Who better than to help protect you from a shady investment than the fraud ninja!

This covert agent is ready with smart investing tips to make sure you don't hand over your hard earned money to some swindler. Watch these short videos to see how the ninja can help you.



[Amateur time](#)

[Affinity Fraud](#)

[Gold Mining](#)

[Oil and Gas](#)

[Timeshare](#)

ANSWERS FOR INVESTMENT FRAUD AWARENESS

These are the answers for the Investment Fraud Awareness Test on pages 8 and 9.

- | | |
|-----|------|
| 1.E | 7.D |
| 2.B | 8.E |
| 3.A | 9.C |
| 4.D | 10.F |
| 5.D | 11.E |
| 6.E | 12.D |

Indiana MoneyWise



Indiana MoneyWise is a financial education program designed to increase financial literacy in Hoosiers and educate them about smart money management and how to avoid being the victim of investment scams. Throughout the Indiana MoneyWise site, you will find interactive learning tools and resources to teach you the skills needed to be both financially fit and a wise investor.

CONTACT US!

Indiana Securities Division
Kelly Griesse
Investor Education Coordinator
302 West Washington Street, Room E-111
Indianapolis, IN 46204
1-800-233-3675

Read back issues of this magazine at www.indianamoneywisemag.com.

Check us out on social media!

