Slide 1

WHILE YOU'RE WAITING FOR THE WEBINAR TO START

WE'D LOVE TO HEAR FROM YOU

Make sure you're connected to audio if you'd like to verbally ask a question. Enter your access code (277.496.459), the pound sign (#), your audio pin (shown on your webinar control panel), and the pound sign (#) again. When we pause for questions, click the Raise Hand icon on your webinar control panel, and we'll unmute your line.

You can also type your questions in the question box on the webinar control panel. When we pause for questions, we'll read those for everyone to hear.

GET TO KNOW OUR TEAM

Brittany Vollmar is a Client Relationship Consultant at Shepherd Financial, providing support and strategic direction to client relationships.

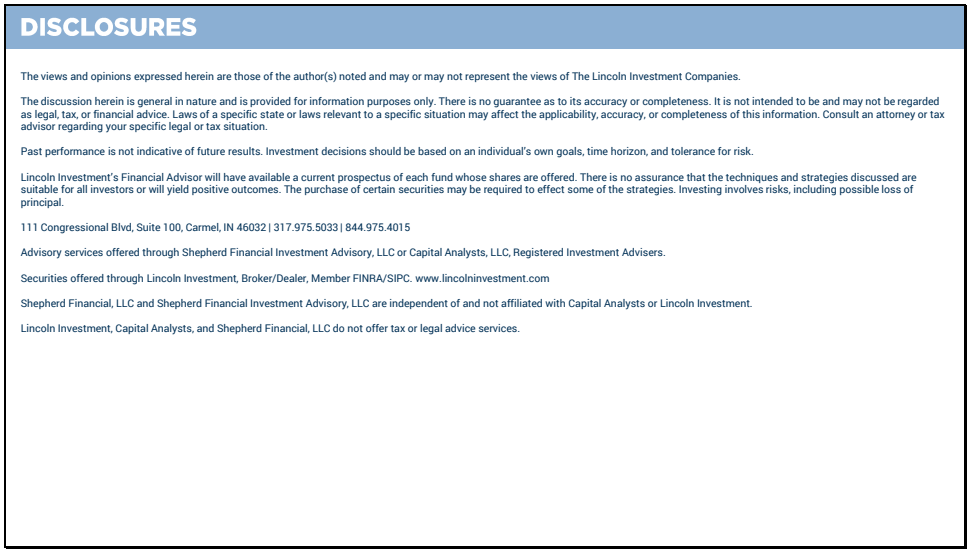
Brittany's favorite flavor of ice cream is coffee.

Holly Willman is the Director of Creative and Strategic Operations at Shepherd Financial. She's been with our team since 2013, utilizing a variety of skills in different roles.

The cicada invasion might be Holly's undoing this summer – she's on sensory overload.

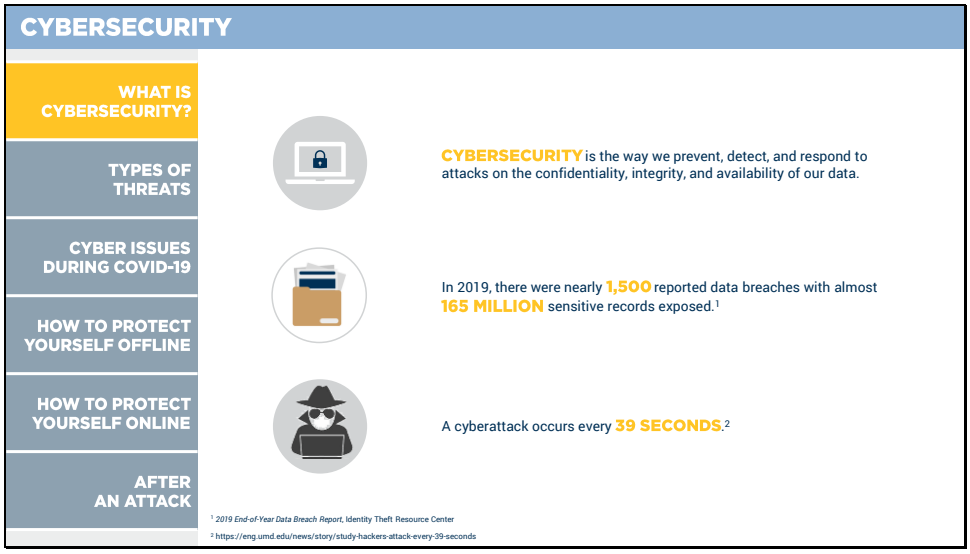
Slide 2

Slide 3



This presentation is for basic investment education. It is not a substitute for reading plan documents, materials provided by fund companies, or materials provided by your employer. This presentation should not be the sole source for your investment decisions, and any performance data quoted represents past performance and does not guarantee future results.

Slide 4



Cybersecurity is the way we prevent, detect, and respond to attacks on the confidentiality, integrity, and availability of our data. There are a number of ways these attacks might come, and they could happen through computers, cell phones, gaming systems, and other devices. The purpose could be financial or political gain, social justice causes, or even cyberbullying.

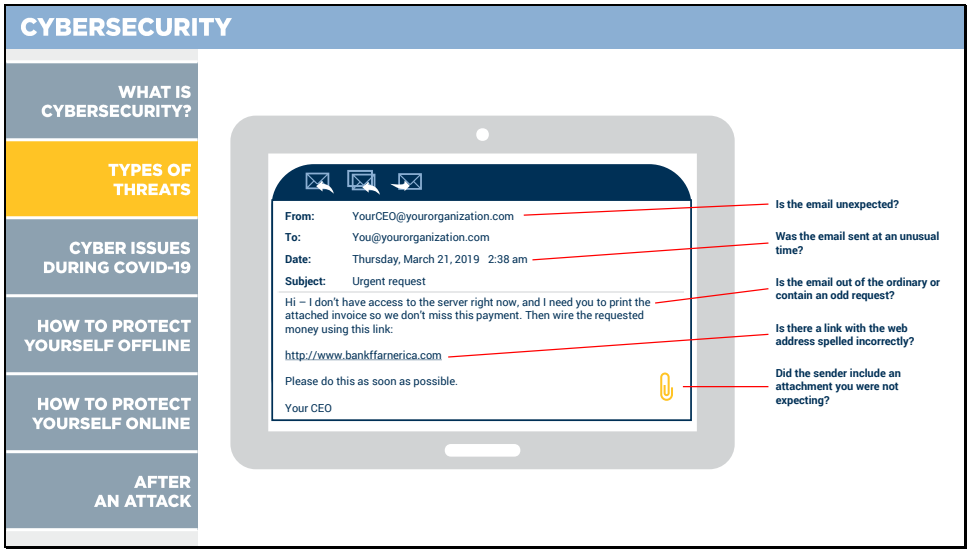
In 2019, there were nearly 1,500 reported data breaches with almost 165 million sensitive records exposed. Worldwide, identity theft is the most common type of data breach incident.

Because so much of the workforce was quickly shuffled to a remote environment, people have been more digitally connected in 2020 and 2021 than ever before. Cyberattacks skyrocketed. The FBI reported last August that the number of complaints about cyberattacks have gone up 400% from what they were seeing pre-coronavirus.

We'll spend some time talking about COVID-specific scams in a minute, but the point is, if you live in the United States, the odds that your data has already been exposed are high. A cyberattack occurs every 39 seconds.

Keep in mind, we are not here to scare you, but we do want to arm you with information.

Slide 5



The term cyberattack is kind of generic, so we'll describe some of the most common attacks and the ways to avoid them. We'll also address what to do if you've been a victim of one of these threats or attacks.

Social engineering is an attack that relies on human interaction to trick users into breaking security procedures and best practices in order to gain sensitive information that's typically protected. Most of the time, this happens because someone is trying to be helpful. An attacker might pose as a coworker with an urgent problem that requires access to network resources. There are many examples of social engineering, but perhaps the most common is phishing.

Phishing is when a scammer uses fraudulent emails or texts – or even copycat websites – to get you to share valuable personal information like an account number, Social Security number, login ID, or even your password. This information can then be used to steal your money, identity, or both. These resemble reputable sources, which is why they might trip you up.

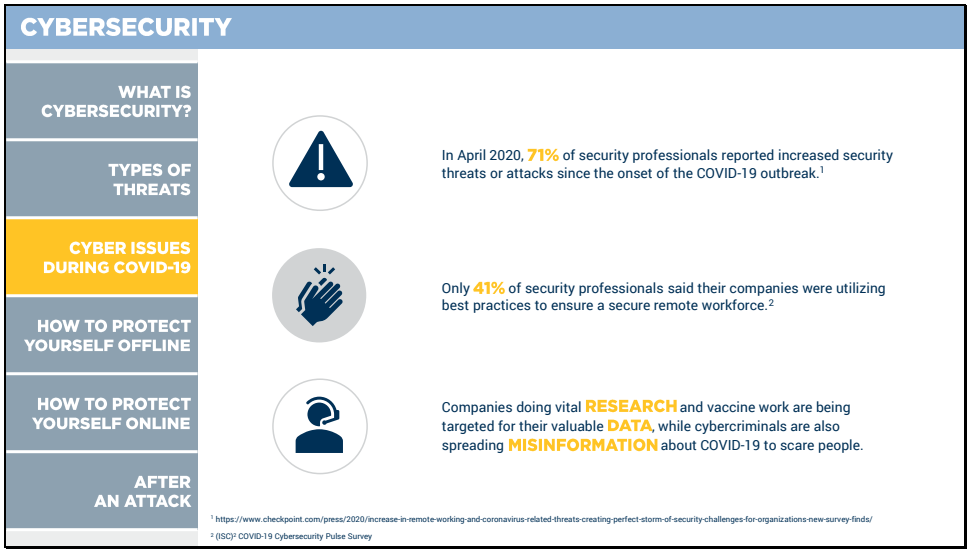
Malware – or malicious software – includes viruses, worms, Trojan horses, spyware, and other unwanted software that gets installed on your computer or mobile device without your consent. These programs can cause your device to crash. Scammers might also use them to monitor and control your online activity. Your computer could become vulnerable to viruses and deliver unwanted or inappropriate ads. Malware is used to steal personal information, send spam, and commit fraud.

Ransomware is a type of malware, and it involves an attacker locking your computer system files. That usually happens through encryption. And then, as the name suggests, they demand a payment to decrypt and unlock them. Unlike other kinds of attacks, the victim is usually notified so that the payment can be made – and that's most often in a cryptocurrency like bitcoin, so the attacker can't be identified.

Finally, tech support scams are very common. The Federal Trade Commission received more than 150,000 reports about these in 2017. A global survey even shows that two out of three people have experienced a tech support scam in the previous 12 months. You might get a phone call, pop up warning, online ad, or a confusing listing in search results. For example, a scammer might call you and claim to be from a reputable company, saying that they found malware on your computer. They might try to get you to install a remote desktop software, and then they would install actual malware on your computer.

And what about pop up warnings? You've probably seen these. They might say your computer is infected and have a number for you to call for help to remove the malware. These can look really scary and very convincing, because who likes to have something urgently telling you there's a problem with your computer? Not me. Your best rule of thumb? Don't click.

Slide 6



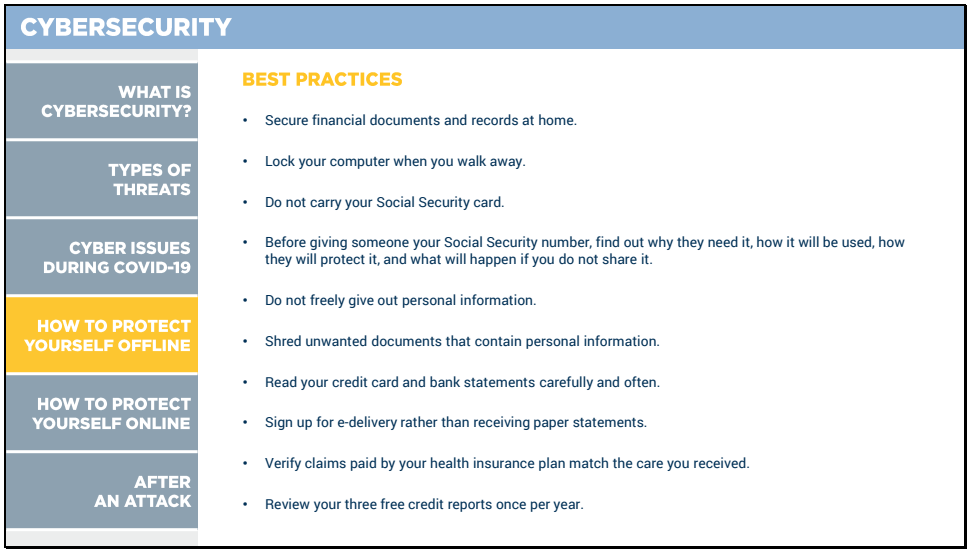
Last April, 71% of security professionals reported increased security threats or attacks since the COVID-19 outbreak. Last May, the 238% increase in cyber attacks against banks was linked to COVID-19. Here's some more unsettling news – only 41% of security professionals said their companies were utilizing best practices to ensure a secure remote workforce. And as a result, we've seen some big companies have some technical difficulties from these cyberattacks – Honda, Garmin, Canon.

Some of the most common forms these attacks are taking during the pandemic are phishing and ransomware. Companies that are doing vital research or vaccine work are being targeted because they have valuable data, and their employees are so busy and stressed so they've become more vulnerable during this time. But there are also hackers and cybercriminals spreading a lot of misinformation about COVID-19 and using text messaging scams to trick people.

Remember last July? There was a social engineering attack on several famous people's Twitter accounts – some big names like Bill Gates, Kanye West, Elon Musk, and Barack Obama. This was done by a 17-year-old hacker in Florida who used traditional hacking, phishing sites, and social engineering. He basically convinced a Twitter employee that he was a Twitter IT employee.

The point is, everyone is vulnerable, and we need to be cautious about our personal data, both online and offline. So why don't we look at ways to stay safe offline?

Slide 7

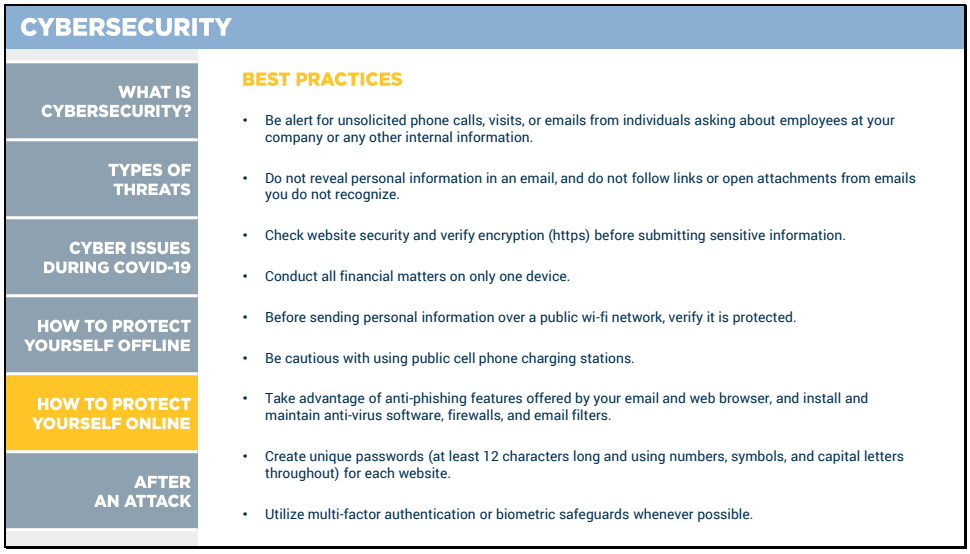


What does it look like to safeguard your information? Start by securing financial documents and records at home. If it's possible, stash your purse or wallet in a safe place at work. And lock your computer when you step away from it. Also, limit what you carry. For example, you should not carry your Social Security card around with you on a regular basis, because your Social Security number is a big deal. If it's always on you, it's easier to steal. In general, if someone asks for your Social Security number, be sure to find out why they need it, how it will be used, how they will protect it, and what happens if you don't share it. Make sure the person gives you a legitimate reason before you share.

Along the same lines, don't give out personal information to just anybody. You want to make sure you know who's asking. Because credit and debit card fraud are so common, it's really important to shred unwanted documents that contain personal information. We don't think about it as much because our lives are so internet-oriented, especially during COVID, but dumpster diving still occurs – people literally go through trash looking for bills, account statements, and other papers with personal information.

Speaking of statements, read your credit card and bank statements carefully and often. If you don't receive a bill when you should, look into it. Make sure claims paid by your health insurance plan match the care you got. And review each of your free credit reports once a year – there are three of them.

Slide 8



Now we'll focus on ways to stay safe online. Remember that social engineering attacks focus on using personal information and posing as someone trustworthy. So be alert for unsolicited phone calls, visits, or emails from individuals asking about employees or other internal information. Don't reveal personal information in an email, and that includes not following links or opening attachments that were sent. If you are unsure if something is legitimate, contact the company by phone, but don't use a phone number from that email. You really want to think before you act – it's suspicious if you're asked to act immediately, offers something too good to be true, or asks for personal information.

Check website security, and make sure it's encrypted before submitting sensitive information. An encrypted site will have https at the beginning of the web address to indicate it's secure. Pay special attention to the URL of a website. Malicious websites may look identical to legitimate sites, but they might misspell the name or use a different domain like .com versus .net. If you hold your mouse cursor over a website link, you may be able to see if it's actually directing you to something else. Be wary of those links! If you know the legitimate website you're trying to access, you can open a new window and type it in instead of clicking the link.

Instead of unsubscribing to spam emails, you should just send them straight to your spam folder. If you hit unsubscribe, you alert the sender that they've hit an active email address, and it could actually result in more spam.

You probably have multiple devices, like a laptop, your phone, a work computer, or whatever. A strong safety recommendation is to conduct all financial matters on only one device – that way you're isolating the number of access points.

I know we all love the thought of free wi-fi, but be smart. Before you send personal information over a public network, see if it will be protected. Speaking of free things, be very cautious with public cell phone charging stations, whether they are at the airport or in your Uber. You don't know what else is plugged into the station that could potentially hack your device. It may be convenient, but it might not be safe.

You definitely want to take advantage of any anti-phishing features offered by your email and web browser, as well as installing and maintaining anti-virus software, firewalls, and email filters to help reduce this unwanted traffic.

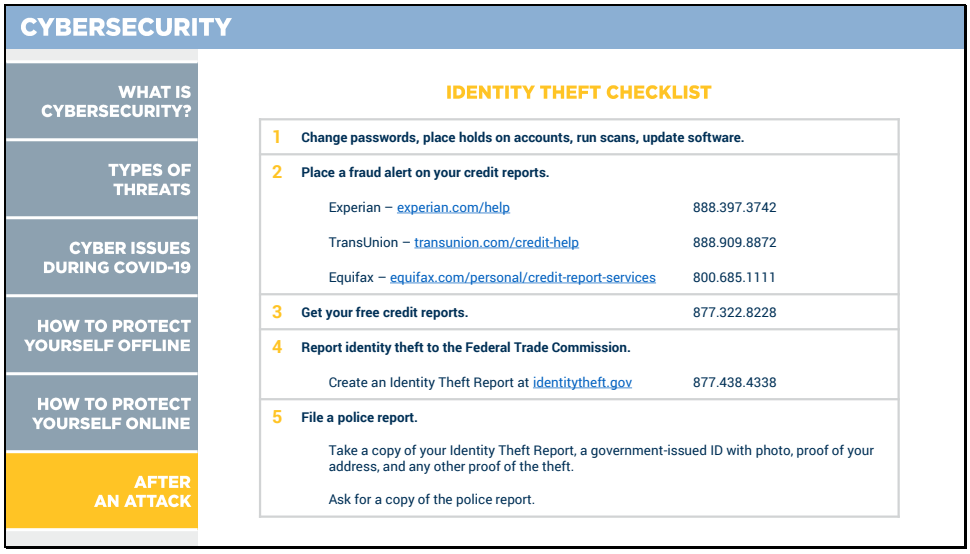
A lot of people treat passwords like a giant nuisance. But here are a few basic rules – don't use the same password for everything. Make it at least 12 characters long and throw numbers, symbols, and capital letters in throughout, not just at the beginning or end. Did you know it's better to have unique passwords for each website than a crazy strong password for all websites? It's called credential stuffing when a hacker figures out that password and uses it to hack all your other sites. If you don't currently use one, consider a password manager. The password vault stores your passwords securely and allows you to use truly random combinations in your passwords, which makes them much harder to crack. And then you only need to remember your master password.

A newer feature that's being incorporated for many websites is two factor authorization or multi-factor authentication. In addition to the password, the second part could be a code sent to your phone or a random number generated by an app or token. Some sites allow for biometric safeguards like fingerprints, facial or voice recognition, or iris scanning.

Remember how we talked about your Social Security number being so important? If someone gets tat number and some other personal information, they can sign up for your Social Security benefits in your name and have them sent to themselves. Not cool. So be sure to create your online Social Security account at www.ssa.gov.

And one more way you can protect yourself is by regularly backing up your files to an external hard drive or cloud storage.

Slide 9



Some warning signs of malware can be found by monitoring your computer for unusual behavior. Is it slower than usual, crashing, or displaying repeated error messages? Is it bombarding you with pop up ads? You also might see new or unexpected toolbars or icons, a sudden or repeated change in your computer's internet home page, or a laptop battery that drains more quickly than it should.

If someone has stolen your information, you might see withdrawals from your bank account you can't explain. Debt collectors might start calling you about debts that aren't yours. The IRS might notify you that more than one tax return was filed in your name or you have income from an employer you don't even work for. If someone uses your Social Security number to file a tax refund before you do, here's what happens: the IRS will reject your filing. Please understand that IRS notices about tax-related identity theft are sent by mail – you will not get an email, text, or social media message from them. And they will not call you with a threat of a lawsuit or arrest.

Protecting your personal information can help reduce your risk of identity theft, but life happens. If you are a victim of a cyberattack, there are some things to do right off the bat. Those include changing your passwords for all online accounts, potentially contacting financial institutions to place holds on your accounts, running scans to make sure your system is not infected, ensuring all your software is up to date, etc.

Let's say someone did file a tax return in your name. When you get a letter from the IRS, follow the instructions and call them using the number in the letter. Use the letter and a copy of your

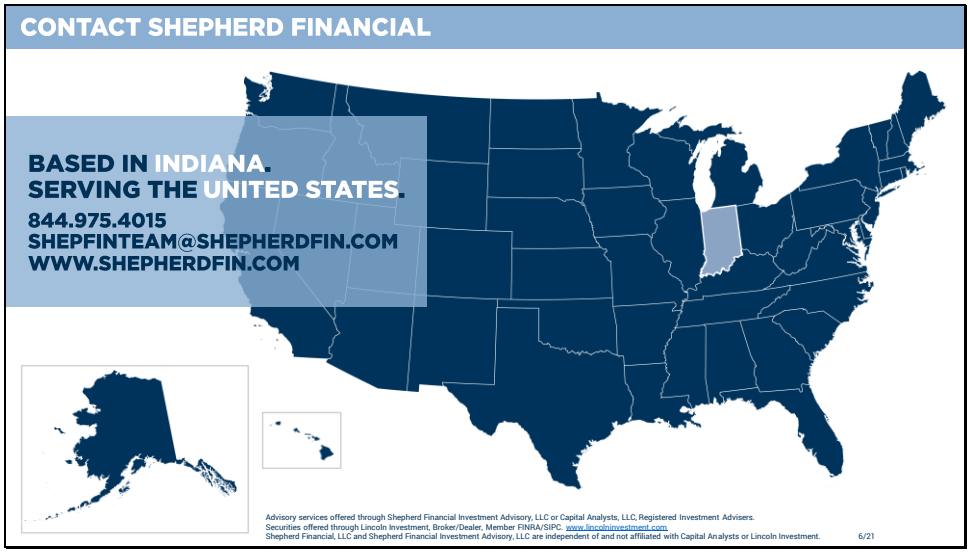
prior year's tax return when you call to help verify your identity. If you think someone used your Social Security number to file for a tax refund but haven't gotten a letter from the IRS, use identitytheft.gov to report it to the IRS and Federal Trade Commission. They will give you a recovery plan.

In this case and other cases of identity theft, you'll also want to limit the potential damage by putting a fraud alert on your credit reports, order your free credit reports, close any new accounts opened in your name, and consider placing a credit freeze on your credit reports. You will likely also want to file a report with the local police. A fraud alert can make it harder for an identity thief to open more accounts in your name. The alert lasts for a year. When you place a fraud alert on your credit report at one of the three credit reporting companies, they must tell the other two.

And when you get your credit report, comb through it for errors. Check the name and address, Social Security number, accounts listed, employment status, information about how you pay your bills, etc. Take a close look at the Negative Information section; this is where you might find late bills or collections. The Inquiries section shows who checked your credit and could be an early warning sign of a problem. A fraud alert allows creditors to get a copy of your credit report as long as they take steps to verify your identity. But a credit freeze locks down your credit. It remains in place until you ask the credit bureau to either temporarily lift it or remove it altogether.

When you go to file a report at the police station, take your identity theft report, a government-issued ID with photo, proof of address, and any other proof you have of the theft. Tell them someone stole your identity and that you want to file a report. Then make sure you get a copy of the police report.

Slide 10


CONTACT SHEPHERD FINANCIAL
BASED IN INDIANA.
SERVING THE UNITED STATES.
844.975.4015
SHEPFINTEAM@SHEPHERDFIN.COM
WWW.SHEPHERDFIN.COM
Advisory services offered through Shepherd Financial Investment Advisory, LLC or Capital Analysts, LLC, Registered Investment Advisers.
Securities offered through Lincoln Investment, Broker/Dealer, Member FINRA/SIPC. www.lincolninvestment.com
Shepherd Financial, LLC and Shepherd Financial Investment Advisory, LLC are independent of and not affiliated with Capital Analysts or Lincoln Investment.
6/21