YANKE FINANCIAL

5540 Centerview Dr, Ste 200 | Raleigh, NC 27606
919-306-5811 | Toll-Free: 800-513-2812 | Fax: 919-375-2303
patrick.yanke@yankefinancial.com
www.yankefinancial.com

A Problem That is Growing Worse over Time

Identity Theft

Patrick H. Yanke, CFP ®
Branch Manager

October 15, 2019

Identity theft is discussed in advertising and the news. Few people really understand its full reach and why it is so hard to combat. It isn't all about credit cards and Facebook. This report is about exposure to the many forms of identity theft. Before we can protect ourselves, we first have to be aware of the risks. This isn't a topic to ignore. The rate of theft is growing exponentially and it will only get worse as more and more of our personal lives become digitized and concentrated in centralized databases. The recent revelations from Equifax show just how vulnerable we all are.

The Problem

- A doctor was arrested for selling prescription medications on the black market. After his arrest and public humiliation, it was determined that his identity had been stolen and someone else was committing crimes in his name--using his medical license to procure the drugs for sale.

- A mother went to enroll her 14 year-old daughter in school and discovered another life. Apparently, her daughter failed to tell her she had been operating a business and paying taxes in Texas for the prior 13 years.

- A family carefully protected their own identity... shredded their sensitive documents and then burning the shreddings! Then, someone filed a fraudulent tax return on behalf of the mother and used that "official" document to open lines of credit, rent vehicles and purchase thousands of dollars worth of computer equipment.

These incidents show the insidious side of identity theft. Two identities were used for criminal activity and the other was more benign--all are major problems for the victims.

Many companies are vying for the chance to be the solution to the problem. However, we are our own first and best solution. There is a great deal each of us can do to safeguard our own identities and protect the identities of family and customers. However, as the third situation showed, there is only so much that can be done individually. The radio ads are right... no one can stop all ID theft--but that doesn't mean we shouldn't try. This is an area where everyone has a part to play and being proactive is key.

Although we hear most about credit scores and financial protections, petty theft through compromised credit cards should actually be the least of our concerns. Direct financial ID theft only accounts for 16% of incidents and is fairly easily recovered compared to other types. We can be reimbursed financially, how do you reconstruct a life?

We're prepared in a world of digital dollars to have to replace our credit cards from time to time when they are compromised. But how do they become compromised so easily? We've been warned to not show our cards as we take them out in the grocery store--there may be unscrupulous people nearby with a camera to record the account number and expiration date. Your server at the restaurant has ample opportunity when taking your card from the table. We've heard about crooks putting card readers over the regular slot on the gas pump to read our cards as we swipe them. These are important areas of concern.

Types of ID Theft in order of occurrence:

- **Medical**
- **Drivers License**
- **Social Security/Tax**
- **Character/Criminal**
- **Financial**

These days, though, point of sale card readers and surreptitious photography aren't necessary for the clever thief. A simple card device from an electronics store can allow anyone to read the last card scanned through a card reader! Despite all of your care during the transaction, the thief may get your information after you have already left the establishment! There is something you can do to protect yourself at the gas pump... the lower left button on the keypad clears the memory (and there may also be a specific "clear" button). You should press this button at the conclusion of your transaction to clear your information. Statistically though, the grocery store is the #1 place where this occurs and there isn't a standard button for clearing the memory.

There is another type of ID theft which is a direct result of our convenience-driven society. In this scenario, a person's address is stolen. How? One way is by simply filling out a convenient USPS postcard online to change your address. For the period of time you don't catch it, your mail (account statements, bills, checks, et al) are collected by thieves and will be used for more invasive actions against you (like filing a fraudulent tax return). Your identity is more valuable to a thief than a simple credit card to swipe.

Another way your address may be compromised is when you become the target for illegal deliveries. For example,

MY BUSINESS PHILOSOPHY

Do unto others as I'd have them do unto me. I don't like to pay people just to have a conversation with them. Let me do a confidential financial review for you. There is no obligation.

ONLINE RESOURCES

My webpage has a wealth of resources and calculators for the online investor. Go to www.yankefinancial.com. Clients can also access their accounts for statements and tax forms.

Continued from the front:

since drug dealers tend to be the shy type, they don't always seek to have their drug supplies shipped to their home addresses... they would rather use yours. They seek homes where packages may remain untouched on the porch for hours after delivery. They simply show up in time to retrieve their items. Imagine being home when they come! Worse still, your kids could be playing in the yard when they come for their illicit goods. This issue is bad for your security in more than one way.

Have a wireless network in your home? It should be password protected to at least a WPA2 standard. There are bad people who drive neighborhoods with their laptop computers looking for unprotected (or poorly protected) networks on which they can conduct their illegal activity. These activities range from illegal forms of pornography to fraudulent financial transactions. When these activities are traced, the authorities will identify your IP address as the source... and you will become the target of prosecutors. Without irrefutable proof, it can be very difficult to prove a negative... that you did not engage in the illegal activities. Your family, your business, and your personal reputation would suffer nearly unrecoverable damage... and you could end up in jail.

Computer viruses are notorious for causing harm to our computers. Did you know these viruses can also be a source of data breach of your personal information? There are viruses which steal your information directly, sure. There are also viruses which are much more insidious... they monitor your typing and identify passwords to give data thieves control of more than what is contained on your computers and home networks. They want your online accounts and profiles. Protect your networks and computers with anti-virus programming and regularly change passwords. It's more than a technical issue.

Many identities are stolen through fraudulent tax returns. Once an identity thief connects your name to your social security number and your birthdate, he has all he needs to file a fraudulent return on your behalf and (as shown in the opening paragraphs) a ticket to everything else. Working together, some thieves have even formed social gatherings where they falsify tax returns in bulk. It's big business... and organized crime.

Similarly, drivers licenses these days are easily obtained by anyone--and often through the internet (especially renewals or reissues). With this basic form of identification, ID thieves do a lot of mischief.

Have you ever printed, copied, or faxed sensitive documents from a business or from home? Recent-model copiers and printers maintain digital information in memory from the documents run through them. When these machines are disposed of they become a very hot item for the black market. In fact, they are one of the most actively sought after discarded items by identity thieves around the world for the information they hold. If you are going to use such a service, make sure the attendants wipe the memory after your use. If it is your own machine, it is up to you to ensure it has been cleared before disposal. This is known as "digital shredding."

Imagine you are in an accident and you are taken to a hospital for emergency surgery. The medications and fluids you will be given will usually be driven by your medical records, if available. What if those records don't reflect your medical history? This happens often--and often with deadly results. Medical ID theft is by far the most frequent form and the quickest way to suffer actual physical harm.

Even when you die, you still won't be free of identity theft. Thieves watch the obituaries for those eligible for government benefits (like Social Security and Medicaid) then assume those identities to keep the entitlement checks flowing--to them. Thieves also assume these identities to open lines of credit, contract for services or gain legal citizenship status. Make sure you notify all relevant agencies when a loved one passes.

Conversely, if your identity has been stolen, it's possible to die before your time. Due to the fraud inherent in government programs, the bureaucracy is very slow to realize a mistaken deaths and restart benefits. In the meantime, those relying on the benefits for sustenance suffer greatly.

Managing the Risks-Individuals

Would you leave $5,000 in your trash or sitting on your desk at work? That is what an ID thief sees when he finds your personal data. Although someone will eventually use your information for some sort of financial benefit, the first benefit a thief realizes is selling your identity on the black market. This won't be the last sale, either. Your identity will be sold and resold multiple times for multiple uses. Your identity is a valuable commodity.

What can you do? The first step is vigilance. Everyone should run a free annual credit report with each of the three main reporting agencies. Go to www.annualcreditreport.com or phone 877-322-8228. It's important to check all three agencies as there are often discrepancies between them. This is a good start for identifying the signs of ID theft (such as unauthorized accounts or new activity in old accounts). There are times when keeping old accounts active makes sense--it can bolster your credit score. However, these accounts should be monitored to prevent unauthorized use.

We all receive those pre-screened credit card and insurance mailings. They present a risk if they are not shredded before disposal. To stop them all together, call 1-888-567-8688. Your social security number will be required. Stopping the mailings can help keep thieves from intercepting and accepting offers in your name.

You can also help others in their duty to safeguard your identity. Much of the following information pertains to businesses and managers. However, knowing what they should be doing for you will help you recognize the signs of risk and correct them. It will also help you, as an employee, understand your role.

Managing the Risks-Companies

Just as suggested for individuals, business owners should also monitor the credit agencies for unauthorized business-related accounts and should consider coordinating with Dunn & Bradsheet on specific business reporting tools. In an age when business entities have lives of their own, they also have identities to protect.

Have you considered carefully who is working for you and their expectations of compensation? Consider that many families are struggling to meet their basic needs. Even some of your lowest level employees have access to sensitive client information... and a potential means to supplement their income. Temptation takes many forms. 55% of ID theft occurs in the workplace. Credit reports are a key tool

in the hiring process... an employee who is a poor credit risk is also a business risk.

You may have trained your workforce well and have a team you can trust. What about the firms which support your business? Can you trust the computer repairman with the IT firm? Can you trust the account manager with the outside firm? What about your seasonal employees? In business, it pays to do your homework and protect yourself.

What can you do to protect yourself and your clients when you hire new employees? One thing you can do is implement a "non-compete" clause in employee contracts. This places legal restraints on employees who might seek to sell your customer information to competitors... or become competitors themselves.

Your business reputation (and your bottom line) takes a hit when you suffer a data breach. Depending on your business, your duty to protect sensitive client data is governed by the Gramm-Leach-Bliley Act, ACTA, and/or HIPAA. You will be held liable for a loss of customer information. Regardless of how you make your money, protecting clients' data should be at the top of your priorities.

Data breaches happen at all levels and some of the most costly recently have come from governmental sources. The South Carolina government was hacked and 3.6 million identities were stolen. Their solution was a year of free credit monitoring for those affected. As mentioned, the financial aspects of ID theft are only the beginning of the potential problems. Consider that each State and the Federal government has access to all of our tax information and much of our personal information. As a result of the Affordable Care Act, they also have a national database of much of our medical information. Future data breaches will be far more costly and broader in application.

Consider Insurance

Businesses and individuals may purchase insurance for identity theft. Individuals need insurance to help them recover from the affects of ID theft and businesses need it to both protect them from liability in a data breach... and to help exposed clients recover. One of the most efficient (and cost effective) insurance sources for individuals is the homeowners policy. Many home insurance companies provide this coverage for a very small premium above the basic policy. There are also companies which specialize in ID theft protection and recovery. Compare literature from multiple sources to find one that most fits unique situations.

We should all take the time to visit with our insurance providers at least annually for a review. Life, family and business situations change... make sure your insurance reflects your current and anticipated risk exposures. Many people conduct an end of year review for this purpose in preparation for the next year. The first step in insurance coverage is also the last... analyzing existing policies and making sure they address risk exposures.

Businesses and individuals should also be cautious on social media (Facebook, LinkedIn, et al). Think about it... data mining really is their business model and the ultimate purpose of these sites. However, they don't know what we don't tell them. As much as the information they gather is useful in their advertising efforts, it's also a treasure trove for identity thieves. It may be fun to let Facebook friends know our birthdates but we are giving away 2/3 of the information needed to file a fraudulent tax return!

Recovery After a Breach

When thieves break into your home, it isn't hard to imagine getting them out and keeping them out. You can change locks, reinforce doors, and install alarms. When thieves take over your identity, they become a part of your life for a very long time. The average time to correct ID theft of any one type is 600 hours. This is where having insurance pays off.

There are two types of identity theft coverage. The first, I mentioned in the previous section. This type of insurance pays for the cost of recovery... but the onus remains on you to do the arduous ground work. The second type actually does the hard work of restoring your identity and cleaning up your credit history. Unless you want to spend 600 hours each on restoring your medical, tax and financial identities (and all of the related ramifications) you should carefully consider this second type of coverage. The two coverages work together... one policy does the actual work of restoring your identity while the other pays the associated expenses.

I highly recommend people balance their checkbooks and review their credit statements every month. In the event your accounts have been breached, you have responsibility to limit the losses. By law, credit cards give you 60 days to correct fraudulent charges before you become liable for them. Although many companies are very good at identifying problems, you are ultimately responsible.

There is no such grace period with bank accounts. Depending on the bank and its policies, a breach of your account which is not the fault of the bank is the client's immediate responsibility. Debit card transactions may be the liability of the cardholder... without a grace period. Make sure you keep an eye on your financial transactions.

At Yanke Financial,LLC, your personal data is sacred. All computer records are encrypted and client files are kept under lock and key. Sensitive documents are cross-cut shredded before disposal. I will not send your personal information through unsecured media (such as email). I follow the guidelines, regulations and protection policies of Raymond James, FINRA, and the SEC in the protection of sensitive client data.

The nature of my business is one of personal relationships. I am the gate through which financial transactions flow. I will never conduct business in your account without a personal conversation with you. Although it may present an inconvenience at times, this is why you can't simply leave messages for me (email, voicemail, et al) to conduct your business. I will always call you back to confirm because I work with people, not numbers.

There is no way to list all of possible methods of identity theft... they are as varied as the people who dream them up. The best we can do as individuals and businesses is to be aware of the risks and insure ourselves in the event of loss. Sadly, it's no longer a question of ***if*** our identities will be stolen but ***when***... and how we will recover when it occurs.

YANKE FINANCIAL

Employer Retirement Plans
Long-Term Care Insurance
Retirement Planning
Education Planning
Risk Management
Wealth Preservation
Charitable Giving
Estate Planning
Life Insurance
Annuities

Capital Markets Review
January, April, July, and October