Three D's of safeguarding your personal data

Ways you can deter, detect and defend

ONE DAY IS TODAY® — FINANCIAL PREPARATION GUIDE

PRODUCTS AND FINANCIAL SERVICES PROVIDED BY THE COMPANIES OF ONEAMERICA®

3 D's of safeguarding your personal data

An estimated 15.4 million consumers were the victims of identity theft in 2016, according to Javelin Strategy & Research, up from 13.1 million the year before. Identity theft and related crimes are on the rise, and they can have a devastating impact on your daily life — and your future. That's because cyber criminals have in their crosshairs more than everyday banking and credit card data — they're also increasingly using identity theft to target the $5 trillion American workers have saved in their retirement accounts.

This issue of the One Day is Today® Financial Preparation Guide focuses on the Three D's of Protecting Your Financial and Personal Information to help you **deter** identify thieves from stealing your personal and financial information, **detect** when your information may be compromised, and **defend** against an attack.

1. Deter identity thieves

How to stay safe online

From ordering food and checking our bank accounts, to keeping up with friends and selling unwanted items, more than ever before, our lives are spent online. But as digital apps and services make our lives more convenient, the risk of identity theft is on the rise, largely because of the bounty of personal information that we freely share online.

What makes that financial information so valuable? It may not take much for cybercriminals to steal your identity, using it to apply for credit, make purchases, pay bills, file a fraudulent tax return and receive tax refunds in your name. Thieves could even take out a home equity line on your house, leaving you responsible for repayment of any money taken and subject to liens on your property.

One of the most important things you can do to ensure your financial future is to protect your personal and financial information today. The following provides some simple steps you can take now to keep your information safe online.

- **Strengthen your passwords.** To decrease your chances of getting hacked, ensure your accounts are properly secured with passwords that do not include personally identifying information and challenge questions that will not be easily guessed. You may not want to use the same passwords for multiple sites. Consider frequently logging into your accounts to ensure information such as address, telephone number and email address, is up-to-date and accurate.
- **Email safety.** We may be used to sending and receiving emails without thinking twice about the type of information we share. Consider avoiding sending credit card information, Social Security numbers or other sensitive information in an email — even if you have high-quality security software installed on your computer or smartphone.
- **Be smart on social media.** Sharing posts and photos with friends and colleagues on social media can be fun; it also can be dangerous. If you post too much personal information, identity thieves can use it to guess your password or answers to security questions. Consider limiting access to your social media and networking sites and don't accept friend requests from people you do not know. And you may not want to share or post personal information online, such as your address, phone number, Social Security number, birth date, or birth place.
- **Secure your phone.** You may want to take advantage of facial recognition, passcode or thumbprint scan options on your smartphone. You could sign up for remote wiping so that you can erase personal information from your phone remotely should it be lost or stolen.
- **Be on the lookout.** Scammers are creating email and/or websites that mimic legitimate banks or businesses in order to steal your passwords, login details and personal information. Phishing email often contains viruses and spyware that can infect your device or capture your passwords or other information, which is why it can be important to keep your antivirus and antispyware software up to date. To protect yourself from these "phishing" scams, don't open files, click on links or download programs unless you verify first that it is coming from someone you know and trust.

What to do if you lose your wallet

There's nothing quite like it – that sense of panic when you reach into your purse or your back pocket and you realize your wallet is missing. To help you take action and limit any potential damage to your credit and your identity, the Federal Trade Commission offers a helpful checklist that could make reporting a lost wallet a lot easier.

How victims' information is misused, 2016[1]

Type of identity theft fraud	Percent
Employment or tax-related fraud	34.0
Tax fraud	29.2
Credit card fraud	32.7
New accounts	25.6
Other identity theft	16.0
Phone or utilities fraud	13.1
Bank fraud[2]	11.8
Loan or lease fraud	6.8
Government documents or benefits fraud	6.6

1. *Percentages are based on the total number of identity theft complaints in the Federal Trade Commission's Consumer Sentinel Network (399,225 in 2016). Percentages total to more than 100 because some victims reported experiencing more than one type of identity theft.*
2. *Includes fraud involving checking, savings and other deposit accounts and debit cards and electronic fund transfers. Source: Federal Trade Commission*

How to keep your personal and financial information safe offline

Identity theft can occur when criminals steal your personal information — your Social Security Number, credit or debit card, checks, bank account numbers, medical insurance or Medicare card, driver's license number, even your address — with the goal of using it to commit fraud in your name.

Not all identity theft is financial. Cybercriminals could steal health insurance information to charge medical procedures to your insurance company under your name. They could use your personal information to apply for government benefits, pursue jobs, rent a place to live, and establish cable and utility services. They could also use your identity when given a traffic ticket or arrested.

You may not have to be online to become a victim. Identity theft can happen anywhere, at a store, a restaurant — even at the office. That is why it may be crucial to protect your personal and financial information in public, at work and even in your own home.

Consider these tips for keeping your information safe offline.

- **Lock it**. You may want to store your financial and medical records, passport, Social Security card and other important papers in a secure place at home. This also could be the place to keep photocopies of the contents of your wallet, including the front and back of your driver's license, credit cards, medical insurance and pharmacy cards, club membership cards, etc., in case it's lost or stolen.
- **Travel light**. When you go out, consider taking only the identification, credit and debit cards you may need and leave the rest at home.
- **Shred sensitive documents**. Thieves could steal information from many sources, including the mail and even garbage cans, and can use it to access your financial accounts. Regularly shred outdated checks and bank statements, credit card applications, medical and other insurance forms, bills, and anything that contains personal

Red flags: Signs that you or a loved one's identity may have been stolen

- Unauthorized charges appear on your accounts
- You see withdrawals from your bank account that you didn't make
- Your credit report shows accounts you didn't open
- You're denied credit for no apparent reason
- Medical providers bill you for services you didn't use
- You get a call or letter about a purchase you didn't make
- Your banking and billing statements don't arrive as expected
- Your credit score changes significantly

information before tossing it into the trash or recycling bin. This includes junk mail such as pre-approved credit card offers.
- **Take it off**. Consider removing or destroying the labels on your prescription bottles before you toss them out.
- **Don't leave a paper trail**. Take ATM, credit card and gas station receipts with you after a transaction. And never let your credit card out of your sight.
- **Watch the mail**. You may not want to leave outgoing or incoming mail in your mailbox unless you can lock it. If you are planning to be away for several days, consider putting a USPS vacation hold on your mail.
- **Get defensive**. Don't assume that you have to give salespeople and others personal information just because they ask. Before you share your Social Security number, birthdate or driver's license number, you may want to ask if it is necessary that you do. Very often, it isn't.

2. Detect suspicious activity

How to keep a close eye on your personal information

Some of the most frequently targeted victims of identity thieves are children and elders. Most kids and many older Americans may not have credit cards or past debts. And because it's unlikely that either would have to run a credit report often, it could be years before an occurrence of identity theft is noticed.

Regardless of your age, recovering from identity theft can be costly in terms of time and money. While keeping a close eye on your accounts won't stop fraud from happening, it can limit the damage that can be done. Here are some tools that can help.

1. **Consider signing up for account alerts**. Many financial service providers, including banks and credit card issuers, offer free online or mobile alerts that can warn you of suspicious activity. Sign up for these alerts whenever possible.
2. **Review your credit card statements**. Check your accounts regularly and make sure you recognize the merchants, locations and purchases listed before paying a credit card bill. If you notice that your bill hasn't arrived, you may want to call your credit card company immediately. And, if you don't need or use department-store or bank-issued credit cards, consider closing those accounts.
3. **Check it out**. Consider reviewing your Social Security Earnings and Benefits statement annually to make sure that no one else is using your Social Security number for employment. You can obtain your statement at www.ssa.gov/myaccount/statement.html.
4. **Order your credit reports**. You are entitled to one free credit report every 12 months from each of the three national credit agencies (Equifax, Experian and TransUnion), which you can order directly from each agency or at www.annualcreditreport.com. Consider spreading out your requests so that you get a report from one of the agencies

every four months, rather than all at once. That way you may have a better chance of quickly detecting any problems that may arise.

5. **Monitor your credit reports**. Check each of your credit reports carefully for accuracy, including your name, address and Social Security number, and for any indications of fraud. If you see credit card accounts you didn't open, applications for credit you didn't complete, credit inquiries you didn't make, charges you didn't authorize and delinquencies you didn't cause, you'll want to setup a fraud alert with the three credit bureaus to put a security freeze on your files and information.
6. **Protect others in your family**. If you're a parent of school-age children, you may want to pay attention to forms from the school, which may ask for personal information, and ask how that information will be used. The Federal Family Educational Rights and Privacy Act (FERPA) gives parents of school-age kids the right to opt-out of sharing contact or other directory information with third parties, including other families. If you have aging parents, especially if they live alone, it may be important to educate them about the dangers of trusting strangers on the phone and the importance of safeguarding personal and financial information at home and when they're out and about.

There is a difference

Credit and debit cards can come with very different protections under the law. Here's what you should know:

Credit card fraud

- If your credit card number (and not your physical card) is stolen, "you are not responsible for unauthorized charges under federal law," according to the Consumer Financial Protection Bureau.
- If your actual credit card is stolen, you are liable for no more than $50 in unauthorized charges — if you immediately report the theft to your credit card issuer.

Debit card fraud

- If your debit card is lost or stolen, and you report it within two business days, you are liable for no more than $50 in unauthorized transactions.
- If you wait to report the loss or theft up to 60 days from the time your statement is sent to you, you could be liable for up to $500.
- If you don't report the loss or theft of your debit card within 60 days after your statement is sent to you, your potential liability is unlimited.
- If an unauthorized transaction appears on your statement but your card has not been lost or stolen, you won't be responsible for the debit if you report it within 60 days after your account statement is sent to you.

3. Defend your rights

What to do if your information is stolen

If you think your personal or financial information has been compromised, get help right away. The sooner a financial institution, credit card issuer, wireless carrier or other service provider is notified that a fraud has occurred, the sooner they can act to help limit the damage — and the sooner you can build a recovery plan to repair your credit, recover your losses, and replace stolen credit and debit cards. The following tips can help you form your plan.

1. **Notify your creditors and financial institutions**. Report any suspicious charges and accounts to the appropriate credit issuers. When you do, you can ask them to close or freeze those accounts so no one else can use them. Consider asking for written verification that the account has been closed and the fraudulent charges were discharged.
2. **Place a fraud alert**. If you spot a sign of identity theft, consider contacting one of the three major credit bureaus (that bureau will pass along your request to the other two) as quickly as possible to initiate a fraud alert on your credit file. This can automatically notify you when anyone tries to open a new account in your name for a minimum of 90 days.
3. **Consider a freeze**. While a fraud alert permits creditors to access your credit report if they take steps to verify your identity, placing a credit freeze with Experian, Equifax and TransUnion (you have to contact each one separately) may provide a higher level of protection by prohibiting anyone, including you, from opening new lines of credit in your name. You can temporarily lift the freeze any time you want to apply for a new loan or credit card; however, you may have to pay a small fee to do so.
4. **Register a complaint with the Federal Trade Commission**. You can report identity theft to the FTC at www.identitytheft.gov. Providing the FTC with an affidavit outlining the specific information that was compromised may not fix the issues you're facing, but your complaint may help the FTC build a case for any wrong doing.
5. **File a police report**. Going on record with your local law enforcement could help with creditors who may want proof that your account was hacked and misused. You may want to keep a copy of your report for your personal records.

Note: OneAmerica is the marketing name for the companies of OneAmerica. Products issued and underwritten by American United Life Insurance Company® (AUL), a OneAmerica company. Administrative and recordkeeping services provided by McCready and Keene, Inc. or OneAmerica Retirement Services LLC, companies of OneAmerica which are not broker/dealers or investment advisors.Provided content is for overview and informational purposes only and is not intended and should not be relied upon as individualized tax, legal, fiduciary, or investment advice. Investing involves risk including potential loss of principal. Before investing, understand that annuities and/or life insurance products are not insured by the FDIC, NCUA, or any other Federal government agency, and are not deposits or obligations of, guaranteed by, or insured by the depository institution where offered or any of its affiliates. • Javelin Strategy and Research, Experian, Equifax, TransUnion and www.annualcreditreport.com are not affiliates of OneAmerica. • Not affiliated with or endorsed by the Social Security Administration, the Consumer Financial Protection Bureau, and the Federal Trade Commission or any governmental agency.

About OneAmerica®

A national leader in the insurance and financial services marketplace for more than 140 years, the companies of OneAmerica help customers build and protect their financial futures.

OneAmerica offers a variety of products and services to serve the financial needs of their policyholders and customers. These products include retirement plan products and recordkeeping services, individual life insurance, annuities, asset-based long-term care solutions and employee benefit plan products.

Products are issued and underwritten by the companies of OneAmerica and distributed through a nationwide network of employees, agents, brokers and other sources that are committed to providing value to our customers.

To learn more about our products, services and the companies of OneAmerica, visit **OneAmerica.com/companies**.

ONEAMERICA®

The companies of OneAmerica®
One American Square, P.O. Box 368
Indianapolis, IN 46206-0368
1-317-285-1111
www.oneamerica.com

© 2018 OneAmerica Financial Partners, Inc. All rights reserved. OneAmerica® and the OneAmerica banner are all registered trademarks of OneAmerica Financial Partners, Inc.

R-29673 03/16/18