FOR IMMEDIATE RELEASE
January 28, 2020

CONTACT: Roman Moniak
(916) 482-2462
rmoniak@rmaintl.org

Your Personal Data Is Your Most Valuable Asset—Protect It

(Sacramento, CA): Tuesday, January 28, 2020 is National Data Privacy Day. It is a day celebrated worldwide as a reminder to all of us that our personal data is an asset worth protecting. Today’s online world of smart phones, Fitbits, Alexa, navigation devices, smart cars, home monitoring systems, tracking devices for your children, and the rampant 24/7 use of social media makes taking steps to protect your personal data more important than ever before.

Think of your personal data as though it is your car. Would you leave it unlocked when you are not using it? Would you leave your car running while you run errands? Would you want the keys to your neighbor’s car to also work for your car? Would you think it is ok for someone else to claim it is your car? The answer to all of these questions is obviously “no.” Yet this is exactly how many consumers manage their personal information. Before you become the victim of identify theft or worse, consider these steps to protect your most valuable asset:

Step #1 Secure your smart phone.

Securing your smart phone is the first step to securing your personal. Smartphones are the gateway into all sorts of data. From work emails to personal messages and information, access to your phone means access into your life. Despite this, 28% of people don’t secure their smartphones with any sort of passcode.

Don’t be one of them! Take the simple step of securing your phone with a passcode, pin, or other security measure, such as fingerprinting or facial recognition. Keep it secure. Keep it safe.

Step #2 Resist the call of password reuse.

The second step to securing your data is very easy. Simply stop reusing your passwords. Passwords are part of all our daily lives. From paying bills to ordering pizza, nearly every web-based interaction requires a login and creation of a password, and therein lies the problem. Because many strings of numbers and letters are needed to create a password, reusing passwords across multiple accounts can seem like an attractive option.

But beware! Password reuse can turn one compromised account into dozens. Take some time to review the passwords you use and consider the following:

• Start using a password manager to wrangle all your various credentials for you.
• Turn on two-factor authentication for your accounts, or at least the most sensitive ones, such as email and banking.

Step #3 Beware phishing emails.

The third step is to avoid responding to any email from a person or company you do not know. One of the most common and most effective ways hackers steal your sensitive data is by luring you into an email conversation with them. Once you are engaged, they can use your email as a gateway to your sensitive data. Personally Identifiable Information, sometimes called PII, is some of the most valuable data that cybercriminals go after.

With a Social Security number and birthdate, an industrious hacker could take control of nearly all aspects of your life, a coworker’s life, or that of one of your clients. With this much at stake, cybercriminals are turning to the keepers of this data—you and your coworkers—to gain access to PII.

Step #4 Don’t let data breaches beat you.

With California taking the lead, laws and regulations are being passed in almost every state to set data protection standards, restrict the use and abuse of consumer data and prevent data breaches. But breaches will continue to happen. The best step you can take to protect the misuse of your data is to place security freezes on your accounts with all of the major credit bureaus: Transunion, Experian, and Equifax. Visit their websites for step-by-step guides to freezing your credit.

Step #5 Realize your devices know each other.

Step five is more of a necessary recognition than a to-do item. All our devices are connected: they know each other and they can share information with each other. More importantly, their connectivity is rapidly expanding. We love our convenient and fun devices, like personal assistants, wearables, speakers, cameras, TVs, cars, home alarm systems, toys, and appliances. But it’s important to understand connected devices rely on and track information about us, such as our behaviors and preferences. Be mindful of when they are on. Turn them off completely when you are not using them and read the privacy practices of companies with whom you share information before you click “Agree.”

For more helpful information, visit the Receivables Management Association International’s website at https://rmaintl.org/consumers/

###

About Receivables Management Association International:

Receivables Management Association International (RMAI) is a nonprofit trade association that represents more than 500 companies that purchase or support the purchase of performing and nonperforming receivables on the secondary market. The Receivables Management Certification Program and Code of Ethics set the global standard within the receivables industry due to its rigorous uniform industry standards of best practice which focuses on the protection of the consumer.

More information about RMAI is available at www.rmaintl.org.