Top Tips for ID Theft Prevention
Individuals

Do

- Sign up for a fraud alert, or better yet a security freeze, on your credit files at all three credit bureaus; sign up for a credit monitoring service; include your kids
- Install an encrypted password keeper on your smartphone and use it, and only it, to manage your passwords; sync with your home computer in case you lose your phone
- Be extra careful with passwords on work accounts, financial accounts and web-based email accounts; use strong, unique passwords; change them every six months; set a reminder in your calendar
- Add a password to your financial accounts so your banks will no longer authenticate you over the phone by your SSN or mother's maiden name
- Set your online banking security settings at a higher level of security than the default (sometimes you can set them to use a second layer of authentication for wire transfers, such as a one-time use pin sent to you by text)
- Find out if your benefits carriers use your SSN as your ID number; if they do, ask them to change it
- Check your benefits cards in your wallet for your SSN (if it is on a card, ask for a new card that omits the number)
- Be suspicious of unsolicited emails asking you to click on a link, download an attachment, or provide account information (beware that the "from" email address of an email you've received can be "spoofed")
- Use firewall and malware protection programs on your computer
- Secure your home Wi-Fi network (this URL has instructional videos on how: www.onguardonline.gov)
- Set your computer's and device's operating systems and apps to receive automatic security updates
- Consult your bank's website to confirm where to download its official mobile application
- Password protect your smart phone, tablet and laptop (if you travel with it)
- Set the privacy settings on your social media accounts; be careful when accepting "friend" or "link" connections on social media platforms to people you don't know
- When you receive a call from a company or organization that seems suspicious, hang up, get their number off of their website, and call them back

Don't

- Consider whether to store your credit card number at the e-commerce sites where you shop—perhaps only those where you shop often; use a strong, unique password; change your password every six months
- Consider not using a debit card for shopping
- Don't ignore your credit card and banking statements; watch out for transactions you don't recognize
- Be careful using P2P file-sharing programs (they can make files on your computer accessible to others)
- Don't set your email program to auto open attachments

Proskauer» Privacy & Cybersecurity

- Don't click inside pop-up windows to close them (instead, use the "X" at the upper right-hand outer corner of the pop-up window to close it)

And If You're Really Serious...

- Create a special email account with your home ISP (e.g., @optonline.net, @verizon.net; not Yahoo!, AOL, Gmail, etc.); use it for your banking accounts only; do not give this email address to anyone but your banks; opt out of all your banks' extraneous (e.g., marketing) emails (this isolates your banking accounts from the malware, phishing and stolen password black market)
- Create a special email account dedicated only for online shopping at sites where you do not store your credit card number (you can also use that email to sign up for coupons); do not use that account for anything else, nor give it to friends or family; only check this account if an order does not show up or you need a coupon code (then, just search for the retailer's name); this account is a repository for spam and scams and should not be used as a communications account; others should be suspicious if they receive an email from this account
- Use website security questions wisely – treat these as a second password on the account; don't use your mother's maiden name as a security question
- Ask your bank for a token for online access to your bank accounts
- Read the "Explanation of Benefits" received from medical insurance companies – look for unfamiliar services rendered
- Compare your annual Social Security Administration statements to your W2s to see if someone else is using your SSN to be employed
- Protect the online accounts you want to keep most secure using multifactor authentication: https://www.socialcustomer.com/2014/04/how-to-enable-two-factor-authentication-on-50-top-websites-including-facebook-twitter-and-others.html
- Be wary of using social media logins to log into other accounts (single sign-on)
- Turn Bluetooth off on your phone when you're not using it
- Disconnect your back up drive from your computer, except a few times a week to back up (to protect your back up from ransomware)
- Periodically check your email account settings (criminals who have hacked into your account can change your settings to forward your email to their own accounts)

To implement a security freeze online, visit the credit bureaus' websites at:

- **https://www.experian.com/ncaconline/freeze**
- **https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp**
- **https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp**

For more information about protecting yourself or your clients, please contact Jeffrey D. Neuburger.

Jeffrey D. Neuburger
Co-head, Technology, Media & Telecommunications Group
Partner, Privacy & Cybersecurity Group
+1.212.969.3075
jneuburger@proskauer.com