THOMSON REUTERS
COMPROMISED CREDENTIALS – FAQS

WHAT SHOULD I DO NOW?

First, contact your IT department or a trusted technology professional. They may have their own standards and practices to further protect you and your data. But we recommend you take the following immediate steps:

1. **SCAN ALL COMPUTERS** – As noted above, speak with your IT professional, but we strongly recommend that you scan your computer for malware or other malicious programs that may compromise your data. This should be done before changing your credentials to avoid having new passwords compromised by the same malware.
2. **UPDATE YOUR ONEPASS PASSWORD** – Even if you were recently asked to change your OnePass password (a forced password reset), or if you have upgraded your system's security, you should still update your password. Information on updating your OnePass password can be found online or contact OnePass Technical Support at 1-800-934-9378 for help. You also should consider changing all other passwords for applications that you use.
3. **UPDATE YOUR MULTI-FACTOR AUTHENTICATION (MFA)** – MFA is a more secure method of accessing and protecting your data, but it too can be compromised, so regularly updating this information is recommended. To update your MFA, you will need to change the password associated with your account, change your security questions and answers, or update the authenticator. Information on updating your MFA methods can be found here or contact OnePass Technical Support at 1-800-934-9378 for help.

WHAT DOES "MY CREDENTIALS HAVE BEEN COMPROMISED" MEAN?

When your credentials have been compromised, it means someone other than you may be in possession of your account information, such as your username and/or password. This can come to our attention in a number of ways. You might identify activity on your account that was not initiated by one of your authorized end users or our security monitoring might pick up activity on your account from an unusual Internet protocol (IP) address. We also partner with trusted third parties that monitor the Web and report to us when customer credentials have been found available on information sharing websites. Many of these sites are not typically accessible to the public, but rather may be part of the "Dark Web" that is frequented by hackers and bad actors looking to buy/sell stolen information.

WHO ARE THESE TRUSTED THIRD PARTIES?

Thomson Reuters collaborates with select public and private security organizations to search for customer credentials and other types of stolen data found on the Dark Web or other information sharing sites. These organizations then provide us with intelligence feeds we can use to report back to our customers and strengthen security protocols.

HOW WERE MY CREDENTIALS COMPROMISED?

While there is no way for Thomson Reuters to know exactly how customer credentials were compromised, most information is stolen through malware installed on a computer used to log in to Thomson Reuters products or websites.

CAN I DO ANYTHING TO MONITOR MY ACCOUNT USAGE?

Yes, you can monitor activity on your account to make sure that searches are initiated by an authorized end user. QuickView+® is a free service of Thomson Reuters that allows you to track usage within your organization.

IS THERE ANYTHING ELSE I CAN DO TO PROTECT MY CREDENTIALS AND DATA IN THE FUTURE?

While your IT department or trusted technology professional may have their own guidance, please consider the following:

- Install updated antivirus software on your computers and update your software when prompted to do so.
- Set your antivirus program to scan your computer immediately upon start-up and to run at all times, including a scan of all incoming emails.
- Don't open unsolicited business emails or attachments that come from unfamiliar sources.
- Look closely at the URL address of a website. Malicious websites may look identical to a legitimate site, but the URL of the malicious site may use a slight variation in spelling or spacing to trick you.
- Manually type the URL address of a website rather than clicking a link. Typing in the accurate URL is a simple way to negate a host of attacks.

THOMSON REUTERS®