NORTHERN TRUST

FREQUENTLY ASKED QUESTIONS

PROTECT YOURSELF FROM "BUGS" AND EXPLOITS

Northern Trust is aware of and monitoring new security vulnerabilities (referred to as "Spectre" and "Meltdown") recently reported by Google Project Zero. These "bugs" have been identified in modern processors manufactured by Intel and other technology companies.

While Northern Trust continues to work closely with technology companies, operating system vendors, and other infrastructure service providers to identify any potential exposure and resolve identified issues promptly, there are steps you can take to help reduce the risk for your home and business.

Technology firms have already begun providing software and firmware updates to mitigate these vulnerabilities, and there are no known situations where the bugs have been exploited.

What is Happening?

"Security flaws", "vulnerabilities" and "bugs" are all essentially words for the same thing – flaws in hardware or software which have the potential to be exploited for malicious purposes. It's important to note that just because a security flaw has been identified doesn't mean that it has been exploited. In fact, it's common that by the time vulnerabilities are disclosed there are already patches and updates available to reduce or eliminate the risk. That's why security experts agree: the best way to keep yourself protected is to keep your systems and software updated at all times.

At Northern Trust, Information Security teams immediately perform an in-depth analysis whenever our sources inform us of a

security flaw. We work quickly to determine any potential susceptibility, and perform comprehensive reviews of existing technical and procedural controls to determine whether gaps or vulnerabilities exist. A similar approach can be taken at your home or business to help determine if you are at risk. Consider the following:

- ***Automatic Updates:*** Is your computer and/or mobile device set to automatically install updates and patches? This is an option that is easy to program and is highly recommended. Patches and updates often contain "bug fixes" that protect against exploits, and ignoring or postponing them puts you at heightened risk.

- ***Up-to-Date Operating Systems:*** Are you running the most recent operating system on your computer and/or mobile device? Sometimes it's easy to postpone an operating system update – whether because of a cost associated with the change or because your mobile device does not have enough memory. While many operating system updates are automatic, there are some that require purchasing the new version (usually only applicable for computers). Keeping the most recent operating system running on your computers and mobile devices will keep your information secure from older vulnerabilities.

- ***Passwords and Encryption:*** Is your home or small business network protected with encryption and a strong password? While not all vulnerabilities are the same, a standard information security best practice involves protecting your network and computers against unauthorized access. Passwords, two-factor authentication, and encryption are all key components of keeping your systems protected against common attacks.

- ***Monitoring:*** Northern Trust is committed to product and client security. In addition to 24X7 monitoring of the digital environment, updates and patches to systems are deployed regularly to reduce the risk of cyber breaches. You can use a similar approach to your home computers by running virus scans on a regular basis and reporting issues when applicable. Virus scans can be programmed to run automatically on a specific day and time, but for best results you should make periodic checks to ensure that if something was found it was fixed.

Questions?

Please refer more detailed inquiries to your relationship manager.