In response to the COVID-19 pandemic, Wolf & Company and WolfPAC Solutions are here to help you with real-time updates, insights, and educational materials to help your organization minimize the outbreak’s impact, and to help you stay prepared for the future. We encourage you to explore our Wolf COVID-19 Resource Center and check back regularly for updated content.

Wolf & Company hosted a webinar on Tuesday, March 31 on the topic of responding to COVID-19 and steps that you can take to continue operations during this interruption. We invite you to listen to the recording and review the presentation for valuable information directly from our experts.

We’re also reading and hearing from regulators about an increase in the risk of unauthorized access and fraud. Last week, Finastra, a core processor, had an outage that appears to be due to ransomware. This increase appears directly related to the rapid deployment of technology and operations to support remote capabilities, which can sometimes result in misconfigured VPNs, significant increase in call center traffic, and elevated phishing and malware campaign levels.

In light of this, we have been helping clients validate that they are maintaining appropriate safeguards and controls through the following remotely executed services:

- Remote penetration testing of VPN appliances and firewalls
- Detailed security configuration reviews of VPN appliances and firewalls
- Remote internal network penetration testing
- Targeted social engineering campaigns
  - Phishing and spear phishing
  - Call center testing
- Business continuity services and pandemic triage and support

We wish everyone well as we navigate this unprecedented situation together. If you have any immediate needs, please reach out to John Doherty at (617) 261-8172 or jdoherty@wolfandco.com.