Treasury and Trade Solutions

Vigilance On Cyber and Fraud Threats

As industries, governments and individuals across the world are responding to the evolving threats associated with COVID-19, cyber criminals are exploiting these events to target institutions to commit fraud and capture sensitive data.

It is important for our clients to know how to counteract risky behavior and stay vigilant about cyber threats. Please work with your Information Security teams and review the tips below for what is best for your organization:

- Understand social engineering risks & follow best practices to stay safe online
- Know what to do when there is fraud or a cyber incident
- Leverage Citi's recommended guidance to clients on cyber/fraud risks

Social Engineering Risks & Best Practices

Please remain vigilant of suspicious activity. Media, security firms and governments are all reporting a steady stream of Corona or COVID-19 themed scams. In particular, beware of emails that claim to provide information on COVID-19, as these could be sent by cyber criminals to entice recipients to open malicious links or attachments.

To help stay safe online, we recommend the following:

- DO NOT click on links or email attachments in unsolicited emails
- DO NOT Forward the message, but do report the suspicious message to your information security department
- DO NOT reveal personal or financial information in email, and do not respond to email solicitations for this information. Contact your Citi representative if you have questions.
- DO use trusted sources – such as legitimate, government websites – for up-to-date, fact-based information about COVID-19.
- DO verify a charity's authenticity before making donations.
- DO review the EUROPOL recommendations for Telework and making your home cyber safe

Payments Fraud & Cyber Incident Response – Speed is of the Essence

- Ensure your staff know their role in response to fraud and cyber events. The Guidance on Combatting Fraud slipsheet is a good start to help prepare your team to be able to spot red flags and mitigate risk. Citi recommends clients review their own incident management processes in light of many changes to work environments in response to COVID-19.
- It is important that all teams are familiar with incident response processes in order to be able to respond promptly during actual or suspected fraud or cyber events. To this end, we recommend familiarizing your staff with the What to Do in the Event of A Fraud slipsheet which provides guidance on key actions to take in the event that your organization experiences a payment fraud or cyber event.

Help Manage Cyber Risk with Preventative Measures

Citi's Cyber Security toolkit provides a range of resources to assist you in your efforts to protect your organization from cyber criminals. We encourage you to leverage these training materials and bookmark this website for information and readiness to respond to cyber and fraud events.

Please feel free to contact us if you have any questions.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions