Important Information: Fraud, Cybersecurity, and Customer Safety

Over the past several months, outlined by media reports and governmental threat intelligence, there has been a significant increase in global financial fraud activities. While these fraudulent activities span nearly every industry, the financial services and technology sectors, in particular, are being targeted. *Therefore, please be alert to fraudsters potentially targeting your business.*

The increased level of fraudulent scams being reported have not just been limited to business email or account compromises. In fact, fraudsters are targeting personal email accounts through sophisticated phishing (email), smishing (SMS/Text), social engineering, and other hacking techniques. These techniques, can and do come in a variety of sophistication levels including:

- ***Servicing & Support Impersonators:*** who will impersonate a trusted third-party and request that you approve or transact account changes or modifications to standard operating or business processes (e.g., additional, or off-cycle payroll runs).
- ***Malware Command & Control:*** to take control of personal or business computers to access banking and business applications, while appearing to be you.
- ***Business Email Compromise & Man-in-the-Middle Attacks*:** to facilitate legitimate email exchanges from your account to others, requesting payments, account changes, personal info, or business modifications.
- ***Fake web-ads on Google, Yahoo*, etc.:** that appear after a web search (see "**Ad**" next to results) to be a legitimate company you are familiar with but redirect your click on the ad to capture credentials or download malware onto your computer.

While there is never a 100% guarantee against becoming a victim to fraud, there are many online resources and guidelines to help protect you, your company and your family. Some of these resources include the Financial Crimes Enforcement Network (FinCEN), the Internet Crime Complaint Center (I3C), the Cybersecurity & Infrastructure Security Agency (CISA), and the FBI's Cyber Unit. Employee training is also key. We recommend making your employees aware and alert to the techniques described above.

Should you ever feel or even suspect that a fraudster is trying to impersonate or represent themselves as isolved, please let us know immediately. Your suspicions may simply be that but in today's environment we believe it is always better to err on the side of extra caution and safety.

isolved wants to assure you that we take the responsibility of securing our systems and safeguarding our customers very seriously and will continue to do all we can to keep bad actors at bay with a combination of partners, people, processes, systems, and training. You can read more about isolved's commitment to security, privacy, fraud prevention and more within the isolved Trust Center.

For more information or to report suspected fraud, please contact your isolved Customer Success Manager or regular isolved contact.

Sincerely,

Todd Atwood, Chief Information Officer, isolved