Socure

New Sanctions, New Risks

Checklist to Ensure Compliance in a Changing Environment

Ensuring Compliance

□ **Ensure sanctions lists are up-to-date.** Examine your update frequencies and review. If your organization is currently reviewing at monthly, quarterly or annual updates you likely need to reassess as frequent changes to the OFAC lists will expose your organization to additional risk of missing a potential hit.

□ **Screen every customer at onboarding.** Ensure that every customer is screened using the most current sanctions list updates to avoid any individuals or entities from entering your portfolio.

□ **Screen every transaction at your organization's transaction risk thresholds.** Re-check existing customers using the most current sanctions list updates before any high value transactions are approved to prevent any last minute activity to circumvent newly issued or anticipated sanctions.

□ **Deploy continuous monitoring of your existing customers.** Enable real-time sanction list updates to allow proactive management of risks in real-time.

□ **Account for multi-jurisdictional issues.** If you operate outside the US across other geographies, assure that those operational alignments and processes are in place. UK, Japan, Australia, New Zealand, the EU, Switzerland and other jurisdictions are applying their own sanctions requirements that will need to be built into operational plans.

Operational Considerations and Steps

□ **Perform an organizational risk assessment.** Evaluate the number of potentially high risk transactions, geographies and business lines. Areas of vulnerability are wires, transfers, commercial accounts due to the UBO challenges, shell companies, etc. Focus on assessing the types of transactions that may involve connections to Russia.

□ **Examine operational areas.** Focus on wires, private wealth and commercial as well as all other LOBs for signs of entities or ties to entities that are sanctioned.

□ **Assess 50% rule for entities.** Any ownership of 50% or more with ties to sanctioned individuals or any other sanctioned jurisdiction or entity must be reported. This would also likely involve a SAR if you are a reporting entity.

□ **Conduct a complete risk program review.** Assess your current program to assure you have the appropriate policies, processes and escalations to support ongoing sanctions changes and priorities

□ **Conduct a cybersecurity program review.** Assess architecture for potential vulnerabilities. Work with your internal teams to assure IP restrictions, security and intrusion testing and capabilities are ready for potential cyber targeting.