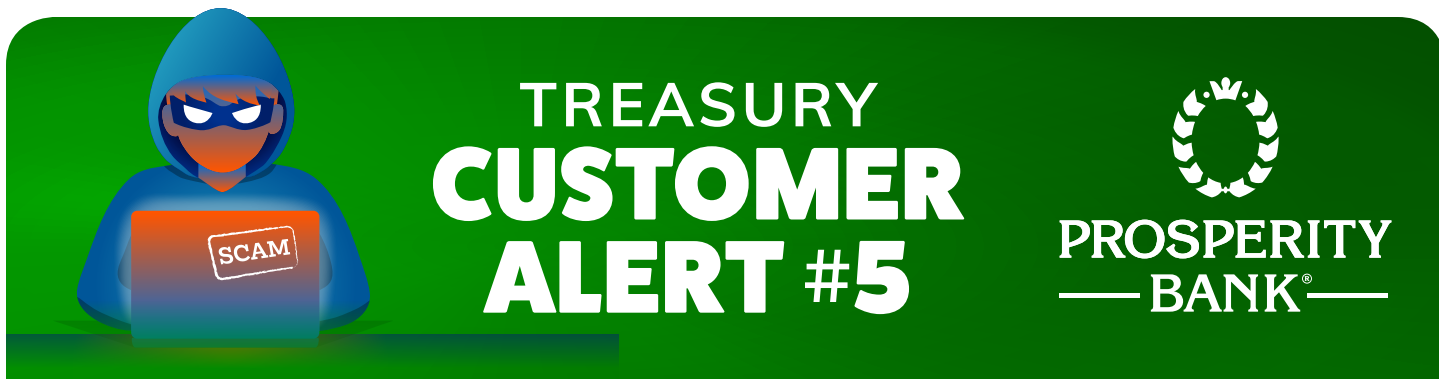




Protect Your Business With Treasury Services

Reduce Fraud Risk. Strengthen Financial Security

Cybercriminals continue to target businesses of all sizes. A single fraudulent transaction can result in significant financial loss and operational disruption.

BUSINESSES SHOULD:

- ◆ Evaluate your current Treasury Services solutions.
- ◆ Review user access and security settings.
- ◆ Confirm fraud controls are properly configured.
- ◆ Ensure employees understand approval and verification procedures.

Treasury Services Tools That Help Reduce Fraud Risk

CONSIDER REVIEWING OR ADDING:

- ◆ ACH Positive Pay
- ◆ Positive Pay for checks
- ◆ Dual approval controls
- ◆ Transaction alerts and notifications
- ◆ Account activity monitoring
- ◆ Wire transfer and ACH payment verification controls
- ◆ A process to verify all payee account changes
- ◆ Multi-Factor Authentication (MFA)
- ◆ Online banking security settings

These tools can help detect suspicious activity before losses occur. However, even the most effective controls require proper configuration and ongoing oversight.

KEY AREAS TO REVIEW:

- ◆ User permissions and access levels
- ◆ Administrator accounts
- ◆ Contact information for alerts
- ◆ MFA enrollment status
- ◆ Approval workflows and transaction limits
- ◆ Outdated or inactive user accounts

REMEMBER:

Small and medium-sized businesses are **increasingly being targeted** because attackers believe they have fewer security controls in place.

Please contact your Treasury Services representative to discuss enhancements to your fraud prevention strategy.



Awareness is your best defense against fraud.



Member
FDIC