



TREASURY CUSTOMER ALERT #2



Fraud Is On The Rise; Is Your Company Prepared?

Caller ID spoofing targeting Treasury Services is a growing cybercrime. Businesses should remain vigilant for this emerging threat! These attackers use caller ID spoofing, social engineering, and publicly available information to appear credible, often referencing real account details or recent activity.

COMMON RED FLAGS OF SPOOFED TREASURY SERVICES CALLS INCLUDE:

- ◆ **CALLER ID APPEARS LEGITIMATE BUT FEELS UNUSUAL** – The number may appear to be from your bank, but spoofing tools can fake this.
- ◆ **URGENCY OR PRESSURE TACTICS** – The caller insists immediate action is required (e.g., “fraud is happening now” or “a wire must be stopped/approved immediately”) to push you into acting without verification.
- ◆ **REQUESTS FOR SENSITIVE INFORMATION** – The caller asks for one-time passcodes, account credentials, or full account details. Legitimate Treasury teams will not request this information over an unsolicited call.
- ◆ **REFUSAL TO FOLLOW STANDARD VERIFICATION PROCESSES** – The caller shows hesitation or resistance when you suggest calling back using a known, trusted number or following internal approval workflows.
- ◆ **INCONSISTENT OR GENERIC DETAILS** – The caller may have partial information but cannot validate specific account details, internal contacts, or prior interactions.
- ◆ **REQUESTS TO BYPASS CONTROLS** – The caller encourages workarounds such as skipping dual approval, using personal devices, or sending information outside approved systems.

While some fraudsters may resist security procedures, others may appear fully cooperative and encourage verification steps to gain your trust. **Never let your guard down simply because a caller seems willing to follow standard protocols.**

RESPONDING TO A SUSPICIOUS CALL:

- ◆ If the call seems suspicious, **hang up immediately**. Cybercriminals want you to stay on the call with them.
- ◆ **Call back using trusted contact information** from your bank’s website, prior statements, or internal directory.
- ◆ **Do not approve** transactions, share credentials, or provide codes during an unsolicited call, especially if there is urgency.
- ◆ **Do not click** on any link sent during the call or follow-up emails. Websites can be spoofed, just like caller ID.

REMEMBER:

Treasury Services will **never ask** for one-time passcodes, passwords, activation keys, or full account credentials.



Awareness is your best defense against fraud.



Member
FDIC