



## Important **Coverage** Reminder to Members

### **MUSIC Social Engineering Requirements**

#### **Please Read!**

Social Engineering Fraud is an intentional manipulation technique that tricks a school employee into paying or transferring money or securities to a cyber-fraudster. The employee believes the request is genuine and submitted by a person claiming to be a vendor, client, or an employee authorized to make the request. Social engineering is one of the most dangerous threats facing MUSIC members. A Social Engineering threat is preventable.

MUSIC will pay up to \$350,000 per Occurrence for a loss sustained by a member, providing they have performed an Official Authorization **subject to the following requirements:**

Before making a wire transfer or ACH payment, the MUSIC member **must** authenticate/verify the request by calling the company or a known representative. Never reply directly to the original email or use contact information, including email addresses, phone numbers, or names contained within the originating request. Your authorization phone call **must** be documented and kept with any wire transfer or ACH transfer records.

**Failure to perform an Official Authorization will void a member's insurance coverage in the event of a wrongful transfer under the carrier, Chubb's, Social Engineering policy guidelines.**