Stripe Security Highlights

1. **PCI DSS Level 1 Certified**
    - This is the highest certification in the payment industry. It means Stripe undergoes rigorous audits to ensure compliance with strict global security standards.
2. **No Sensitive Data Stored on Your Servers**
    - Stripe handles card numbers and sensitive payment details directly, so your organization (and HOA Start) never stores or transmits card data. That dramatically reduces your risk exposure.
3. **Data Encryption**
    - All payment data is encrypted in transit (TLS/SSL) and at rest. Card numbers are encrypted with AES-256, and decryption keys are stored separately.
4. **Tokenization**
    - Stripe uses tokens in place of raw card numbers. That means even if a database was compromised, no usable credit card information would be exposed.
5. **3D Secure 2.0 & Strong Customer Authentication (SCA)**
    - For certain transactions (especially international ones), Stripe supports multi-factor authentication to help prevent fraud.
6. **Radar for Fraud Protection**
    - Stripe includes machine-learning fraud detection (called *Radar*) that looks at billions of data points to flag suspicious transactions.
7. **Global Compliance**
    - Stripe complies with GDPR, PSD2, and other regional security and privacy regulations, which is especially important for communities with members outside the U.S.

How are payments kept secure?
We use **Stripe**, one of the world's leading payment processors, to handle all online transactions. Stripe is trusted by millions of businesses worldwide and meets the **highest level of security certification (PCI Level 1)**.

- All payment information is **encrypted** and processed securely.
- Sensitive card details are **never stored on our servers**.
- Stripe's advanced **fraud detection** helps protect your community from suspicious activity.

This means your members' payments are handled with the same security standards used by major companies like Amazon, Shopify, and Lyft.

Stripe Support