Security and Fraud Prevention: How Stripe Protects Your Transactions in How Many Strokes Online Rental Manager

How Many Strokes ApS
Empowering Golf Clubs with Seamless Rental Solutions
Date: October 7, 2025

Introduction

At How Many Strokes ApS, your trust is our top priority. Our Online Rental Manager is designed to streamline golf equipment rentals, enabling your golfers to make payments or reserve credit card details for future charges directly through your app. We act solely as the interface between your operations and Stripe—no funds ever flow through our company. All transactions are processed securely via your own Stripe account, ensuring you maintain full control and compliance.

Stripe is a global leader in payment security, employing cutting-edge technology to detect and prevent fraud, including attempts with fake or stolen credit cards. This document provides an overview of Stripe's robust security measures, tailored to our shared ecosystem. By leveraging Stripe's tools, we help safeguard your business from fraud while delivering a frictionless experience for your golfers. For more details on Stripe's security practices, visit Stripe's Security Overview (https://stripe.com/security).

Stripe's Overall Approach to Credit Card Security and Fraud Prevention

Stripe prioritizes proactive fraud detection to combat unauthorized card use, especially in card-not-present (CNP) transactions common in online rentals and subscriptions. Global card fraud losses exceeded $28 billion in 2021, with U.S. e-commerce businesses facing $3.75 in costs for every $1 of fraud—a 20% rise since 2019. Stripe's strategy includes secure processing via tokenization and encryption, EMV chip technology for in-person elements (if applicable), and verification checks like Address Verification System (AVS) and Card Verification Value (CVV).

For recurring charges—like golf rental reservations—Stripe monitors patterns to flag anomalies, such as unusual small transactions that could indicate testing. Businesses using Stripe benefit from reduced chargebacks and revenue protection, with tools that adapt to evolving threats without disrupting legitimate payments.

Stripe Radar: AI-Powered Fraud Detection at the Core

Stripe Radar is our integrated, no-code fraud prevention solution, powered by machine learning trained on over $1.4 trillion in annual payments from millions of global businesses across 197 countries. It scans every transaction using hundreds of signals—from device fingerprints and IP proxies to historical patterns and card network data—assigning real-time risk scores and automatically blocking high-risk payments.

Key Features for Fraud Handling:
• Real-Time Blocking: Radar identifies fake credit cards and card testing by detecting rapid, anomalous patterns. It blocks these before they succeed, reducing fraud by an average of 38%.
• Adaptive 3D Secure: For high-risk transactions, it prompts extra verification without excessive friction for genuine users.
• Sophisticated Signals: Includes proxy detection for IP spoofing, cumulative risk scoring, and integration with Visa, Mastercard, and American Express for early alerts.
• Custom Rules and Insights: Tailor rules for your golf club specifics.
• Dispute Prevention: Automatically resolves disputes via Verifi and Ethoca.

Radar learns from Stripe's vast network—giving a 92% chance a payment pattern has been observed before—making it more accurate than standalone tools.

Specific Protections Against Fake Credit Cards and Card Testing

Card testing involves fraudsters using bots to test stolen card validity on merchant sites, often via high volumes of low-value attempts. Stripe combats this head-on:

• Detection and Automated Blocking: Radar flags patterns like rapid failed charges or mismatched device data.
• Verification Layers: Mandatory CVV and AVS checks prevent incomplete or fake submissions.
• Platform Mitigations: In our Online Rental Manager, we implement Stripe-recommended integrations to collect rich data.

If testing is suspected, Stripe enables immediate transaction freezing and reviews to halt activity.

How Many Strokes ApS • Larslejsstraede 1 • DK - 1451 Copenhagen K.
+45 7239 1000 • info@howmanystrokes.com • VAT: DK-40013776

Page | 2

Best Practices for Your Golf Club's Stripe Account

To further fortify your setup:
• Enable Radar Fully: Review rules in your Stripe Dashboard.
• Rate Limiting: Set transaction caps.
• CAPTCHA and Endpoint Restrictions: Restrict automated attacks.
• Monitoring: Use Stripe's analytics to track patterns.
• Training: Educate staff on spotting disputes tied to fraud.

These steps, combined with our interface, ensure minimal false positives for legitimate golfers.

Conclusion

With Stripe's AI-driven defences and our secure integration, your Online Rental Manager transactions are protected against fake cards, testing, and broader fraud risks. This layered approach not only prevents losses but also builds confidence for your golfers, encouraging repeat rentals.

If you have questions or need help configuring your Stripe settings, contact us at support@howmanystrokes.com or your account manager. Together, we're driving secure growth for golf clubs worldwide.

Best regards,
The How Many Strokes ApS Team

This document is for informational purposes only and reflects Stripe's publicly available security features as of October 2025.

How Many Strokes ApS • Larslejsstraede 1 • DK - 1451 Copenhagen K.
+45 7239 1000 • info@howmanystrokes.com • VAT: DK-40013776

Page | 3