CREDIT CARD AUTHORIZATION

How it works

The Intuit Customer Profile Management module securely stores your data off-site, eliminating the need to re-key or store account your data on paper or in our computer systems. It's simple, safe and secure.

Protection of Cardholder Data and Customer Data

Intuit has implemented various measures, including appropriate administrative, technical and physical safeguards, designed to ensure the security and confidentiality of Cardholder Data and Customer Data, protect against anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information. Such measures may include, among others, encryption, physical access security and other appropriate technologies. Intuit continually reviews and enhances its security systems, as necessary. Intuit is subject to the detailed rules and regulations of the various credit and debit card organizations and networks (i.e. VISA, MasterCard, American Express, NYCE, Star, etc.), relating to the security and safeguarding of Cardholder Data, including, but not limited to, the Payment Card Industry Data Security Standards ("PCI"), VISA Inc.'s Cardholder Information Security Program ("CISP") and MasterCard International's Site Data Protection Program ("SDP"). Intuit endeavors to comply with all such rules at all times. Pursuant to such rules and regulations, Intuit is required to undergo periodic third-party assessments and periodic network scans to ensure that, among other things, Intuit has installed and maintains a firewall configuration to protect data; does not use vendor-supplied defaults for system passwords and other security parameters; protects stored data; encrypts transmission of Cardholder Data and sensitive information across public networks; uses and regularly updates anti-virus software; develops and maintains secure systems and applications; restricts access to data to those with a business need-to-know; tracks and monitors all access to network resources and Cardholder Data; regularly tests security systems and processes; assigns a unique ID to each person with computer access; restricts physical access to Cardholder Data; and maintains a policy that addresses information security.

Authorization

By signing below, I authorize **SEEBERGER DERMATOLOGY, LLC** to collect my credit card data for storage and future use. I understand that the data will be stored only by the affiliated third-party, secure, PCI compliant credit card vendor, Intuit and that the information will not be stored by **SEEBERGER DERMATOLOGY**, **LLC** at any time.

By signing below, I acknowledge that SEEBERGER DERMATOLOGY, LLC reserves the right to charge a fee if I do not show up for my procedure appointment.

This payment authorization is for the products and/or services provided to me by **SEEBERGER DERMATOLOGY, LLC**. **Any unpaid balances after 30 days from receipt of insurance explanation of benefits will be charged to the credit card on file.** I certify that I am an authorized user of this credit card and that I will not dispute the payment with my credit card company for *professional services* after those services have been actually rendered.

Patient Name (printed): _____

Signature: _____   Date: _____