Information Security Privacy Policy – C2

Updated 2/20/2019

We Protect Your Privacy
Protecting your privacy is important to us. We hope the following statement will help you understand how we collect, use and safeguard the personal information you provide to us on our website and as a cardholder.

Security - When confidential personal account data is sent to us through the Internet (Onboarding), we require that a "secure session" first be established using Secure Socket Layer encryption technology (SSL). Our internal security standards safeguard your information submitted by computer in several ways. Encryption helps protect your data from interception by a third party. Except for access to data by authorized personnel or the sponsor of your card program required to conduct business, you will be the only person accessing your data (Onboarding process). We use security techniques designed to protect our customer data -- especially when certain data is used by employees and business partners to fulfill customer services.

Information Collection - Our website, during the onboarding process, may request that you voluntarily supply us with personal information, including your E-mail address and other sensitive KYC information, for purposes such as identify verification, enhanced due diligence, or participating in voluntary online surveys. We limit the collection of information about our customers to what we need to know to facilitate the onboarding process, to provide customer services, and to fulfill any legal and regulatory requirements. We use advanced technology and well-defined employee practices to help ensure that customer data is processed promptly, accurately and completely. Our employees are permitted access to only the information they need to perform their jobs. This data is gathered during onboarding and stored securely. We maintain strict internal policies against unauthorized disclosure or use of your information. Each authorized employee is personally responsible for maintaining consumer confidence in the company. We provide training and communications programs designed to educate employees about the meaning and requirements of these Customer Privacy Principles. We conduct reviews of our compliance with the privacy principles and the specific policies and practices that support the principles. Employees who violate these principles or other company policies and practices are subject to disciplinary action, up to and including dismissal. Employees are expected to report violations -- and may do so confidentially -- to their managers. C2 performs annual SOC2 and PCI audits to remain at the highest level of compliance.

Information Use –If you provide us with your E-mail address, or have done so in the past, we may upon occasion send you information by E-mail. We will not use your information in any way shape or form or share it with any third-party providers or solicitors. This email list is used to send you information will be developed and managed under strict conditions designed to safeguard the security and privacy of customer information.

Aggregated and De-identified Data is data that we may create or compile from various sources, including but not limited to accounts and transactions. This information, which does not identify individual personal or business information, may be used for our business purposes, which may include offering products or services, research, marketing or analyzing market trends, and other purposes consistent with applicable laws.

Linked Internet Sites – None of the C2 Portals incorporate 3rd party linked sites.

Customer Privacy Inquires
INFO@ICCE.EMAIL

Updates to this Privacy Policy

This Privacy Policy is subject to change. Please review it periodically. If we make changes to the Privacy Policy, we will revise the "Last Updated" date at the top of this Notice. Any changes to this Notice will become effective when we post the revised Notice on the Site. Your use of the Site following these changes means that you accept the revised Notice.