

EBizCharge Security



EBizCharge[®]
BY CENTURY BUSINESS SOLUTIONS

Table of Contents

Introduction	3
Organizational Security	4
Payment Security	5
PCI.....	5
TLS 1.2.....	5
Encryption.....	5
Tokenization.....	5
Servers, Backups, and Recovery.....	6
Fraud Prevention Modules.....	6
Third-Party Security Scanners and Assessors.....	7
Azure.....	7
Multi-Factor Authentication.....	7
Identity and Access Management.....	7
Password Security.....	7



Introduction

Our mission is to facilitate simple and efficient payment transactions for companies and their customers. The security of these transactions is of the utmost importance, which is why we maintain the highest security qualifications available and put rigorous protocols in place, including TLS 1.2 and multilayered tokenization and encryption.



Organizational Security

EBizCharge security starts at an organizational level. Our Chief Security Officer (CSO) leads our security team and oversees our risk management and vulnerability management programs. Our CSO holds CISSP, Security+, Network+, CySA+, CASP+, CSAE, CSAP, Cloud Essentials, CyberSec First Responder, and CyberSafe certifications.



Payment Security

EBizCharge is dedicated to securing the sensitive digital elements that fuel payment acceptance. By combining multi-layered security screening and proactive account monitoring with the latest tokenization and encryption technologies, we continue to be on the forefront in preventing cyber fraud.

PCI

EBizCharge helps our customers remain PCI compliant by ensuring sensitive payment information undergoes several levels of encryption and tokenization and storing it offsite. Additionally, we offer customers resources that provide further education and self-assessment.

We are certified as a Qualified Integrator and Reseller (QIR) by the PCI Security Standards Council.

EBizCharge is HIPAA compliant and protects patient health information with HIPAA-compliant features such as data tokenization and EMV capabilities.

TLS 1.2

All communications and processing in EBizCharge occur through Transport Layer Security (TLS) 1.2. EBizCharge uses a 2048-bit RSA key and does not support cyphers known to be weak or vulnerable.

ENCRYPTION

All sensitive data undergoes several layers encryption using the strongest and most up-to-date protocols, including AES256 encryption and SHA2 signatures.

TOKENIZATION

Our system tokenizes sensitive information once it has been encrypted, assigning a random replacement value that is impossible to decipher. This process ensures all customer data is safe, even in the case of a security breach.



SERVERS, BACKUPS, AND RECOVERY

Our server farm consists of essentially 100% virtual servers on Dell VRTX chassis, and we are a Microsoft Hyper-V farm. Our credit card processing scope is offsite in the Microsoft Azure Cloud Space.

We use high-availability failover clusters for business continuity management of server outages. EBizCharge performs incremental and differential backups on premises, and we push data to an offsite repository for disaster recovery.

FRAUD PREVENTION MODULES

EBizCharge employs fraud prevention features that are built on a module stack design. Each module controls a different aspect of security so that merchants can choose which modules to include in the fraud control stack. Some examples of modules include: duplicate transaction control, block by country, block by IP address, and many more. The module stack design provides the opportunity for merchants to add or change their fraud modules depending on their unique security needs. We're always adding new fraud modules to the EBizCharge payment gateway to keep our merchants up to date with the latest fraud security.

Our fraud prevention modules also allow merchants to apply different fraud settings to different keys or sources. For example, a merchant may wish to implement a high level of fraud control for an online shopping cart, but a lower level on the console for their own employees.



THIRD-PARTY SECURITY SCANNERS AND ASSESSORS

EBizCharge uses multiple third-party security companies to ensure that our security always meets the strictest of industry security standards. Every security assessor working with EBizCharge provides us with a certification so that our clients can know that we meet security standards.

AZURE

EBizCharge uses Azure for our credit card processing environment.

MULTI-FACTOR AUTHENTICATION

We use Security ID, Username and Passwords (3-layers) to authenticate users.

IDENTITY AND ACCESS MANAGEMENT

Admins can define user roles across accounts in order to restrict certain rights, such as Admin User rights.

PASSWORD SECURITY

To recover or reset their password, EBizCharge users are required to correctly answer security questions or connect our support team directly.

