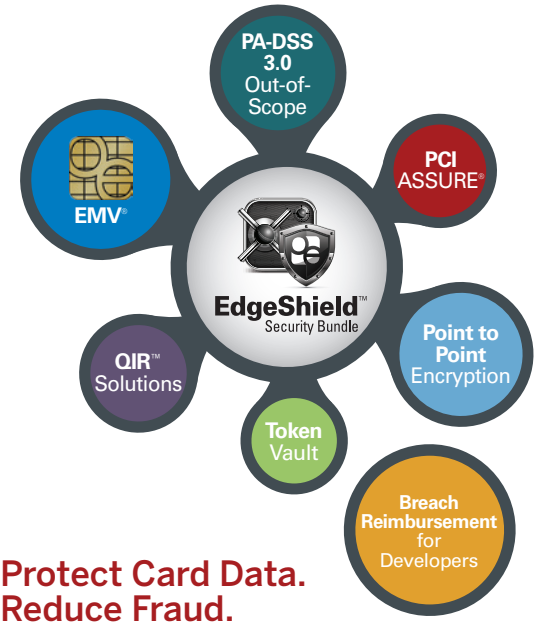
openedge
A division of globalpayments

Practice
MANAGEMENT SOLUTIONS

Developer Solutions

EdgeShield from OpenEdge



Protect Card Data. Reduce Fraud.

855.443.8377
developers@openedgepay.com
openedgepayment.com/practice-management
blog.openedgepayment.com

PaymentsIntegrated. Innovative. Intelligent.

A proprietary bundle of complementary, EMV®-ready security solutions to deliver one of the industry's most secure payment platforms for practices

Cardholder data breaches have become a serious issue among big-box retailers and small businesses, alike. Since 2004 – despite complex PCI requirements – more than **1 billion records** have been compromised, raising concerns about the health of digital commerce. A data breach can be a significant liability for a developer offering payments functionality, not to mention the impact on merchant operations.

OpenEdge maintains that the most effective method for keeping cardholder data safe is a **multi-pronged approach**, combining EMV®, encryption and tokenization. **EdgeShield™** is the OpenEdge answer – an **advanced security services bundle** intended to protect credit card data, prevent counterfeit fraud, and enhance payment processing security. Through a unique collection of complementary security solutions, EdgeShield delivers one of the **industry's most secure payments platforms** while aiding practice management developers and practices with EMV. When integrated into systems that accept payments, the bundle protects credit card data while at rest and in transit.

Included with EdgeShield™

THE OPENEDGE EMV SOLUTION

This fraud-reduction technology protects card issuers, merchants and consumers from losses due to the use of counterfeit and stolen payment cards at the point-of-sale. EMV smart cards are embedded with a chip that interacts with a merchant's point-of-sale device, ensuring the card is authentic and belongs to the user. This chip technology is virtually impossible to duplicate. The technology helps insulate developers from complex device driving and card brand certifications.

P2P ENCRYPTION

OpenEdge's proprietary encryption is designed to render cardholder data unreadable, encrypted at the device. Merchants are unable to view card numbers after the swipe or hand-key.

TOKEN VAULT

Cardholder data is replaced by digital "tokens" based on this technology. Sensitive data is stored in the secure OpenEdge vault rather than in the merchant environment.

PA-DSS 3.0 OUT-OF-SCOPE

Payment applications are rendered out-of scope with EdgeShield, eliminating cumbersome PCI validation requirements.

OPENEDGE SOLUTIONS FOR QIR™

The latest requirements from the PCI Security Standards Council state that small businesses must have their payment applications and terminals installed by Qualified Integrators and Resellers (QIRs). These security professionals are trained and certified to install and maintain PA-DSS validated payment applications. OpenEdge will help you navigate the QIR™ requirements, whether you need access to certified installers or plan to get your staff certified.

OpenEdge: QIR Certified

The security experts at OpenEdge have achieved QIR certification and can ensure your small business merchants are using payment applications installed and serviced in accordance with PCI standards.

Get Certified: QIR ASSIST

For developers who wish to pursue QIR certification, OpenEdge offers QIR ASSIST, a support program to get your staff certified and ensure you have access to payments security best practices. QIR ASSIST includes:

- Consultation with PCI security experts
- Education on topics such as: secure remote access, malware prevention, encryption and tokenization
- QIR exam preparation
- Post-certification marketing assistance to promote your new status as a Qualified Integrator and Reseller

PCI ASSURE®

EdgeShield includes the PCI ASSURE® program to help merchants simplify PCI compliance with online access to security self-assessment questionnaires, network scans, and custom security profiles generated from the business' processing activity.

BREACH REIMBURSEMENT FOR DEVELOPERS

OpenEdge can cover up to $150,000 in legal costs associated with a developer's defense against a customer in the unlikely case of a card data breach while using EdgeShield.

Merchant Breach Example

There is no "typical" data breach scenario. Cyber-thieves access merchant credit card processing systems in sophisticated, unexpected ways, often skimming sensitive cardholder data for months. Here's an example of how one business was affected by a recent data breach:

Industry: Medical practice
Breach method: Network sniffer planted on server
Time until discovery: 7 weeks
Records compromised: 450

Associated costs:

- Lost business
- Detection
- Escalation
- Customer notification
- Remediation
- Fines
- Legal fees

Total price tag for breach: $46,000

Data Breach Statistics

openedge
A division of globalpayments
OpenEdge is pleased to be a **certified QIR organization.**
PCI Security Standards Council
QUALIFIED INTEGRATORS AND RESELLERS (QIR)™ PROGRAM

Sources: OpenEdge, Payment Card Industry Security Standards Council

OEPracMgmtEdgeShield-SD-080717-TN