KeyBank

Cybercriminals target credit card processing:

Protect your business from merchant account fraud

The security of your credit card processing systems and your customers' financial data is integral to the health of your business. These systems are increasingly under attack from cybercriminals who use sophisticated methods to access valuable account information. Being a victim of fraud can be costly — both to your business's bottom line and to its reputation. Be aware of threats to your business and put measures in place to deter fraudsters.

How fraudsters are attacking

Taking advantage of vulnerabilities in your system security, fraudsters will hack merchant accounts to run authorizations to test the validity of card details they have stolen or purchased on the dark web. These fraudulent authorizations can result in an onslaught of fees to you that are charged by the card brand networks. Once they've verified data, fraudsters also use stolen credit cards to pay for goods and services, which can result in charge-back risks to your business.

How you can reduce the risk of fraud

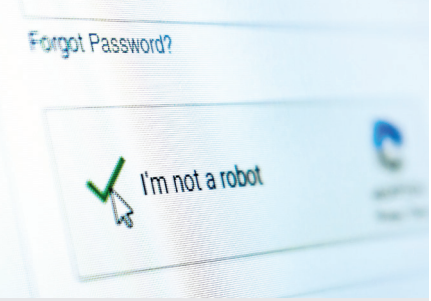
You should implement a layered approach to secure your credit card systems and reduce the risk of fraud. No single tactic can completely stop fraud; however, adding multiple layers of protection can make it more difficult for criminals to reach valuable data or make fraudulent charges before they're detected.

Best practices at the credit card terminal

- Know your customer: Check customers' IDs or obtain contact information when possible.
- Swipe or use the EMV chip as much as possible.
- Use Address Verification Services (AVS) during each sale if the card is not present.
- Enter the three- or four-digit Card Verification Value (CVV) whenever possible.
- Ensure your customers can easily get in touch with you in the event they are dissatisfied with the product or service provided.

Best practices for your merchant gateway and e-commerce systems

- Make sure you set CVV and AVS filters.
- Use velocity thresholds to limit the number of transactions permitted within a specified time frame, including HTTP session velocities, which limit the number of operations per user session.
- Maintain firewalls that include basic tools for botnet detection, prevention, and removal, or more sophistical tools like Network Intrusion Detection Systems (NIDS), rootkit detection packages, network sniffers, and specialized anti-bot programs.
- Employ CAPTCHA, visual challenges designed to distinguish humans from automated scripts.
- Device fingerprinting with proxy piercing capabilities is a code designed to identify multiple contacts with the same device, along with technology to detect the originating device in the case of a botnet.
- Anomaly detection identifies sudden or unusual spikes in traffic to your webpage or unusual patterns in shopping or form entry behaviors.
- Set time out parameters to cause online sessions to expire after periods of inactivity.



- Cross Site Request Forgery (CSRF) detection alerts when unauthorized commands are submitted from a user that the web application trusts.
- Add data validation for guest checkouts, if you allow them.

Many of these measures don't significantly change your customers' experience, but they provide necessary enhanced security that keeps their account information safe and your business financially sound. In addition to these technology solutions, we recommend your business explore options for cyber fraud insurance. If you believe your business has experienced fraud, alert your financial institutions and insurance carrier as soon as possible, and report to local law enforcement and the Internet Crime Complaint Center (IC3.gov) for online fraud.

How Key helps you manage and secure your customer payment data

Fraudsters are continually adapting their methods to gain valuable payment information. To help protect your organization and your customers, KeyBank Merchant Services and KeyBank Information Security and Fraud collaborate to keep you informed of trending criminal tactics and offer actionable ways to prevent and combat fraud.

To learn more:

For more information on how to keep your business information secure, please visit us at Key Merchant Services or key.com/cybersecurity.