HANCOCK WHITNEY®

Your Dream. Our Mission.

Questions about fraud safeguards?

Visit **hancockwhitney.com** to review **Your Payments Acceptance Guide and Dispute Management Best Practices.**

We are committed to protecting your business from credit card fraud.

As a valued merchant services customer, we promise to periodically provide you with critical information to help you prevent unnecessary risks to your business, including encouraging you to review your card acceptance practices and safeguard against card fraud.

Your e-Commerce website is always open 24/7, 365 days a year. When customers pay for goods or services on your website, they are making a card-not-present (CNP) purchase, which means you, the merchant, were not presented with a physical credit card by the cardholder. That's why CNP transactions are more susceptible to fraud.

Fraud can occur at any time, whether you're accepting card present or card-not-present payments. There are some warning signs that can help you and your associates identify potential fraudulent activities.

Be aware of customers who:

- Purchase a large amount of merchandise, then cancel a portion and request a refund via a money order or cash;
- Request overnight/rush shipping to an address that is different than the cardholder's billing address;
- Are first time shoppers and communicate via email/text only;
- Process abnormal transaction amounts;
- Process dozens/hundreds of transactions with similar card numbers; typically, for small amounts, such as $0.01.

According to the **True Cost of Fraud Study** from LexisNexis Risk Solutions, every $1 of fraud loss actually costs a company $3.13.[1] This is partially due to transaction fees, chargeback fees, losses from goods and declined sales due to decreased customer confidence. Small businesses that become victims of cyberattacks rarely bounce back from the damage. In fact, 60 percent of small to midsized businesses close their doors within six months of being hacked.[2]

By implementing the six safeguards listed on the next page, you can help detect early warning signs of possible fraud in your credit card processing and decrease the likelihood of fraudulent transactions and chargebacks.

Please remember to review payment card acceptance best practices outlined in Your Payments Acceptance Guide and Dispute Management Best Practices. These comprehensive, easy-to-read guides are available to you to download, view or print free anytime at hancockwhitney.com.

If you do believe a transaction is fraudulent, please contact your Merchant Services Customer Support Team at **504-299-5114** or **MerchantServices-Support@hancockwhitney.com** as soon as possible.

[1] "Study Preview Finds Cost of Fraud for E-Commerce Merchants Highest Ever," CardNotPresent.com, 6 June 2019.
[2] "60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself," Inc., 7 May 2018.

Six ways to minimize your e-commerce fraud risk.

To help protect your business from e-Commerce fraud risk, here are six best practices you should consider:

1. **Enable Fraud Protection Tools**
   Depending on the payment gateway you use to accept online transactions, you have access to fraud protection tools. At a minimum, these filters should be enabled, if applicable:

- Velocity filter – prevent card runners from testing cards on your accounts

- Card Verification Value (CVV) filter – require customers to enter the 3- or 4- digit code on the back of the card (on the front for American Express)

- Address Verification (AVS) filter – verify that the billing address and zip code provided during the transaction match what the issuing bank has on file

- Unmatched Refunds – stop refunds from going back to cards that didn't have the original sales charged to them.

2. **Use CAPTCHA with Hosted Payment Form**
   When cardholders checkout on your website, they are asked to identify a combination of distorted letters and/or numbers or asked to classify pictures to complete the transaction. This is known as CAPTCHA – Completely Automated Public Turing test to tell Computers and Humans Apart. Pairing this method with your hosted payment form provides an extra layer of security that helps reduce your risk of counterfeit transactions and protects bots from infiltrating your website.

3. **Maintain PCI Compliance**
   Any merchant storing, processing, transmitting, or affecting credit or debit card information must adhere to and comply with the standards set forth by the Payment Card Industry Security Standards Council (PCI SSC). These standards were established to help ensure the security of customers' credit card data within merchants' payment environments, including e-Commerce websites. Regardless of your card acceptance method, PCI Compliance is an on-going process for every business that accepts credit and debit cards.

4. **Keep Platforms and Software Up-to-Date**
   Cybercriminals use tools to detect sites with unpatched applications. By keeping your website and backend software updated with the latest security patches, you reduce the risk of exposing vulnerabilities to potential hackers. Additionally, install and regularly update anti-malware and anti-spyware software developed for businesses.

5. **Monitor Transactions and Reconcile Accounts Daily**
   It's not enough to only review your transactions and accounts on a weekly basis. You may check on Friday and by Monday something's gone awry. Fraud happens daily, and that's why you need to look for suspicious transactions, such as small amounts or mismatched shipping and billing information. Staying on top of this and notifying Hancock Whitney Merchant Services as soon as you notice something out of the ordinary will help minimize any potential damages.

6. **Stay Educated on the Latest Fraud Tactics**
   It's easier to combat fraud when you know what you're up against. Cybercriminals are always searching for new ways to thwart technology and invade your payment environment. Stay on top of the latest news by subscribing to industry journals, e-newsletters, or blogs and be sure to check out Hancock Whitney Merchant Services Customer Resources page.

Hancock Whitney Bank, Member FDIC. All loans and accounts subject to credit approval. Terms and conditions apply.