

Convenience, Security, Trust



Your 1-2-3
Combination for
Fraud Prevention

Visa works for you

Visa[®] Business cards provide convenience and security—whether you're streamlining your bookkeeping, controlling employee spending, or monitoring expenses. More convenient and cost-effective than cheques or cash, your card is a safe form of payment that can save you time and money.



At Visa, we take security seriously and provide solutions, technology, and guidance to help combat card fraud, card misuse, and spending outside policy.

Card Fraud occurs when an unauthorized user purchases goods or services using a business card.

Card Misuse occurs when an employee uses a business card to make a personal purchase and claims the purchase as a legitimate business expense.

Spending Outside Policy occurs when an employee uses a card for business purchases not allowed by the organization (e.g., buying from an unauthorized supplier).



What is Visa doing to help prevent fraud?

Visa and its Member financial institutions work hard to stay a step ahead of fraud. As your business resource, Visa has developed a multi-layered strategy—combining technology and cardholder education—to help reduce the risk of fraud at every step of the transaction process.

Card Verification Value 2 (CVV2): This three-digit number imprinted on the back of your Visa Business Card adds another layer of security to reduce fraud in card-not-present transactions, such as the phone or Internet. CVV2 and its use in the authorization process help prove that the person ordering goods has the card in his or her possession.

Address Verification Service (AVS)*: This service is used to verify a cardholder's billing address, as part of the authorization request, to help ensure that the cardholder is indeed the person who is making the purchase.

Neural Networks*: These software systems monitor and compare transactions to thousands of previous legitimate *and* fraudulent transactions. Based on these comparisons, the neural networks can help identify and stop fraudulent transactions *as they enter* the payment system through the authorization process.

Education: Visa is committed to keeping cardholders informed of the latest fraud techniques and prevention guidelines, as well as reinforcing the importance of immediately reporting lost or stolen cards.

Skimming is an illegal act to obtain card account information. Typically, a card is swiped through a reader that copies information from the card's magnetic stripe. The information can then be transferred onto a counterfeit card. Visa is helping to combat this tactic by embedding a microchip in future cards, providing an additional layer of security over the magnetic stripe.

Phishing is an online scam where fraudulent websites mimicking those of legitimate businesses—such as a bank or a popular online merchant—are set up by criminals to obtain card accounts or other personal information from unsuspecting web users. Be wary of replying to junk or “spam” emails, which can contain links to phishing websites. Also be on the lookout for spelling errors or other inconsistencies, which can be dead giveaways. Visa has worked with organizations such as the Better Business Bureau, Microsoft, and eBay to help identify and shut down phishing sites, as well as with government and law enforcement in public and media education.

* May not be supported by all Visa-issuing financial institutions.

What can **your business** do to help prevent fraud?

10 best practices to improve your card program security

Complementary to Visa's anti-fraud technology is our commitment to cardholder education and awareness. We've developed a step-by-step Best Practices guide to help small and medium businesses build a well-managed, efficient, and safeguarded card program.

Manage the Card Program

1. Select someone to manage the card program; ideally an employee who isn't a cardholder, to avoid potential conflicts of interest
2. Instruct your bookkeeping or accounting staff to watch for suspicious card activity
3. Create a way for employees to confidentially report suspected card abuse

Develop Card Program Policies (for organizations with multiple business cards)

4. Determine which employees require cards, and make sure to cancel cards when cardholding employees leave the organization
5. Train your employees on acceptable card use, and have them sign a cardholder agreement

6. Develop guidelines for card use, such as a list of approved suppliers and limits for monthly transactions, and enforce the consequences of card misuse
7. Require original receipts for every card purchase made
8. Review total card spending on a regular basis to ensure that policies are followed

Put Technology to Use

9. Integrate card purchases into your accounting system to develop a full picture of company spending
10. Leverage reporting software to identify unusual card activity



Secure with Visa

Trust is at the heart of Visa's business, and protecting *Visa* cardholders—with technology, solutions, and guidance—is a top priority. For more information on how you can further benefit from Visa's evolving anti-fraud services, visit visa.ca/smallbusiness or contact a *Visa*-issuing financial institution.

Canadian Imperial Bank of Commerce

1-800-465-4653
www.cibc.com/ca/small-business

Laurentian Bank

1-800-522-1846
www.laurentianbank.ca/en/enterprises/pme

RBC Royal Bank**

1-800-769-2520
www.rbcroyalbank.com/business/small-business

Scotiabank

1-877-552-5522
www.scotiabank.com

TD Canada Trust

1-800-9TD-VISA
www.tdcanadatrust.com/tdvisa/commercial.jsp

Visa Desjardins

1-800-266-5662
www.desjardins.com/business_card



Small Business. Big Possibilities.™

™ Trademark of Visa International Service Association; Visa Canada Association is a licensed user.

® Registered trademark of Visa International Service Association; Visa Canada Association is a licensed user.

**RBC and Royal Bank are registered trademarks of Royal Bank of Canada.

