

FACT SHEET



security

Staying Ahead of Fraud

Today's data thieves are sophisticated in their technological prowess and in their understanding of payment infrastructure. They are smart, nimble and determined — moving quickly to take advantage of new opportunities to perpetuate fraud globally.

To meet this threat, every entity with a stake in electronic payments must be fully committed to protecting the system. The fundamental trust that customers place in their choice of payment is at stake. At Visa, we believe nothing is more important than security and building trust among all stakeholders in the system.

Multiple Layers of Security

There is no “silver bullet” that will erase fraud. Visa's approach is based on the belief that the only effective way to fight fraud is to employ multiple layers of security. Criminals attack the payment system from many directions, using multiple tools and tactics. From anti-counterfeit measures to neural networks that analyze each transaction in real time, Visa takes a total-systems approach to fraud prevention.

Fighting Fraud

Visa has invested heavily in advanced fraud-fighting technologies, and we continue to develop and deploy new and innovative programs that fight fraud and protect cardholders. Visa's efforts have kept fraud rates at historic lows, enabling cardholders to use Visa with confidence. In fact, with technological innovations and advances in risk management, fraud rates have declined by more than 50 percent in the past decade.

Layers of Defense

Visa's processing network supports multiple defense layers to prevent network intrusions, protect against account fraud and to render stolen card data unusable for criminals. Those defense layers include data encryption, sophisticated intrusion detection and fraud monitoring tools capable of analyzing each transaction in real time.

Advanced Authorization

With Visa Advanced Authorization, when a Visa card is swiped, our network can provide an instantaneous rating of that transaction's potential for fraud to the card issuer. The ability to “see” all VisaNet transactions in real time helps stop fraud at the checkout counter — before it takes place.

New Technologies

Chip technologies add an important security layer to transactions, bringing convenience and speed to cardholders and merchants, and Visa supports the rollout of chip technology globally. Future security schemes are likely to involve the authentication of dynamic data — data that changes with every transaction in an effort to further foil fraud.

Online Authorization

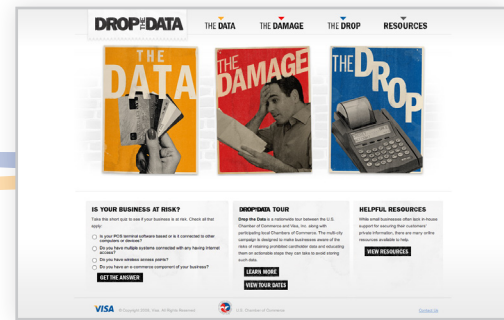
Visa employs several tools to help online merchants avoid fraud for payments where the card is not present at the point of sale. This additional layer of security helps prevent unauthorized online use before it happens.

Empowered Cardholders

Visa empowers cardholders to take an active role in managing their spending and protecting their accounts. VisaNet can provide near real-time transaction alerts and notifications by e-mail or text message whenever a registered Visa card is used for a purchase or to withdraw cash from an ATM — often arriving while the receipt is printing. Such alerts can provide cardholders with a warning of unauthorized use, limiting the potential for fraud or stopping it altogether.

Strength Through Partnerships

As an industry leader, Visa creates an environment of partnership, fosters broad engagement and promotes accountability around securing sensitive consumer data. We work hand in hand with the larger payments community, from cardholders to merchants, financial institutions to service providers, regulators to law enforcement. Our collective success in maintaining the trust and confidence of consumers comes from this ability to work together, share information and coordinate our defenses.



Strong Partners

In 2006, Visa led the industry's establishment of the Payment Card Industry Security Standards Council (PCI SSC), an open global forum to maintain data security standards wherever card data is stored, processed or transmitted. The council is a cooperative effort to align payment network security requirements under a single framework. To encourage all participants to secure cardholder data, we have implemented incentives to promote standards compliance. More than 95 percent of the largest U.S. merchants have validated compliance with PCI SSC

Collective Success

For small businesses, Visa partnered with the U.S. Chamber of Commerce to encourage merchants to eliminate storage of prohibited data through a national education campaign called "Drop the Data." Additionally, Visa developed security standards for payment application vendors to support merchants to reduce data storage and provide more secure payment application products.

Education and Alerts

Visa issues periodic security alerts on emerging fraud trends and actionable steps on how to mitigate against them. That information is further disseminated through educational outreach efforts, including seminars and webinars.

Educating Consumers

In addition to working with industry to secure the payment system, Visa is proud to work with key partners to bring additional education and resources to cardholders. We launched a campaign with the Better Business Bureau to educate consumers on how to identify phishing scams, avoid becoming a victim and report suspicious e-mails. For the cardholder who suspects he or she may already be a victim of identity theft, Visa works with Call for Action to provide consumers with free and confidential assistance through a toll-free hotline. We also joined the U.S. Postal Inspection Service, the National Consumers League and other industry organizations to sponsor an educational campaign about check, money order and wire transfer scams