Partner with us

We partner with clients to help them find the right balance of risk and reward, security and convenience to maximize the value of their cardholder relationships. Through quarterly optimization performance reviews, we provide our partners with a comprehensive suite of benchmarking on fraud, authentication, recovery and other risk metrics, including insights on actionable areas of opportunity to maximize legitimate transactions and minimize fraudulent ones. We provide support in case of ecosystem data breaches and other adverse events, focusing on quick event response and resolution.

The world of payments is changing fast. More digital, more access, more opportunity, and more risk. While managing risk is part of everyone's job at Visa, it's our team's full-time job.

Our mission is to enable growth by sustaining trust in the Visa payment system.

We partner with our clients and governments to anticipate risks and find solutions that enable people everywhere to pay and be paid with confidence.

For more information on Risk Management, please reach out to your Visa Account Executive.

Visa's Risk Management

Trust is the cornerstone of Visa and a critical factor in driving business growth for Visa and for our clients.

As a payment leader, our goal is to make Visa the safest way to pay and be paid for everyone, everywhere. We do this by:

Risk Management
Mitigating risk to the payments system

Payment Security
Advancing an industry roadmap to enhance the security of the system

Trusted Voice
Serving as a trusted voice on security issues with clients, merchants, consumers and regulators

Risk Advisory
Leveraging our risk expertise to help clients mitigate risk while achieving business goals

1 Risk Management

Visa operates a suite of programs to protect the safety and soundness of the payments ecosystem. These programs focus on maintaining compliance with legal and regulatory requirements, restricting illegal transactions in the Visa system, protecting the system from bad actors, and driving compliance with industry risk management and security standards. These programs include:

Data Security and Third-Party Risk:
Develops data security standards and policies; manages programs that promote increased adoption of security standards and solutions by clients, merchants and third parties to protect vulnerable data; implements strong agent oversight and controls around third-party processors.

Credit Settlement:
Protects the ecosystem from the impact of a client's failure to settle obligations; monitors the financial condition of individual countries and financial institutions and sets collateral requirements.

Franchise Risk Management:
Sets and implements brand protection policies and programs; engages acquirers to address brand-damaging merchant activity, including transactions used to purchase illegal goods; engages policymakers on issues impacting their jurisdictions; works with clients to address excessive chargeback and fraud activities.

Anti-Money Laundering:
Reviews all new license applicants, including non-financial institutions and new Visa initiatives; works with clients to correct inadequate AML controls.

2 Payment Security

Securing the payments ecosystem requires continuous investment and innovation in new technology and collaboration with our business partners. Our job is to partner with our clients to make it harder for criminals to succeed and to strive to ensure consumers and businesses believe that their Visa products remain the safest way to pay and be paid. Our security pillars are:

Removing Sensitive Data: As long as data remains valuable to criminals, they will pursue it, and data breaches will continue. By rendering sensitive payment data useless, we're reducing the criminal incentive to steal it in the first place. This is accomplished, in part, through the deployment of two technologies: EMV chip and tokenization.

Protecting Data: Deploying new technologies across all channels around the world will take time and, in some cases, the data may never be fully removed. We must reinforce our efforts to prevent the data from being stolen in the first place by adhering to the highest data security standard established by the Payment Card Industry (PCI) Security Standards Council and encouraging the adoption of point-to-point encryption technology.

Harnessing Data: Just as data is critical to the criminals' success, it is also an important element of our efforts to improve authentication and detect breaches. We are driving the industry away from the use of knowledge-based authentication that uses easily compromised, skimmed or phished information such as mother's maiden name and PIN to more secure measures that use identity, device or dynamic information such as biometric data, dynamic passcodes or device identification. We also continue to invest in advanced data analytics to enable issuers to make more informed decisions on behalf of their Visa cardholders and more quickly identify and respond to data breaches.

Empowering Consumers: Consumers are an important element in the fight against fraud. If consumers can see account activity in real time, set parameters for how their accounts are used, and decide how their information is used for fraud detection, we can unlock the power of consumers to stop fraud. These efforts include transaction alerts, spend controls and mobile geo-location.

3 Trusted Voice on Security

Visa supports global and local market security initiatives by actively participating in industry forums, hosting security conferences, and engaging with local payment groups to both share our risk expertise and gain input from our partners. Through forums such as the Payment Card Industry Security Standards Council, EMV Co, Merchant Risk Council, and International Anti-Counterfeiting Coalition, Visa helps guide and develop standards, share best practices, discuss evolving security trends, and promote collaboration on inter-regional risk issues.

4 Risk Advisory via Risk Management

Share expertise and provide support on the following:

- Fraud and authentication trends
- Benchmarking fraud and authorization performance against peers
- Best practices and guidance on new risk technologies
- Implementation of data security compliance programs
- Resolution of ecosystem breach incidents
- Updates on payment fraud schemes impacting clients
- Deployment of Visa risk tools and solutions
- Updates on local regulatory developments