



## Visa Issuer Privacy Principles

In the course of opening accounts and providing services for individual Visa cardholders, Visa Issuers are entrusted with information related to cardholders' accounts. This information is vital to each Issuer's ability to provide cardholders with quality services, products and opportunities that are tailored to their individual interests and qualifications. Visa recognizes, however, the reasonable expectation of privacy that cardholders may have concerning aspects of this information, and recognizes the importance of respecting and protecting the privacy of Visa cardholders.

Accordingly, Visa has adopted these privacy principles with the expectation that they will serve as a foundation upon which Issuers will build their own privacy policies, tailored to their particular needs and circumstances. By adopting these principles, Visa and Visa Issuers will continue their leadership in the financial services industry and will continue to respect and protect the trust and confidence of Visa cardholders.

### **Principle One: Recognize Cardholder Privacy Expectations**

**Issuers should recognize and respect the privacy expectations of Visa cardholders.**

Consumer privacy is an important public concern. Lou Harris surveys have found that American consumers express a general concern about the use of their information, and how technology is used to collect and distribute information about them. Visa recognizes the importance of this issue to cardholders and the important role it plays in their trust and confidence in Visa and Visa Issuers. Accordingly, the Visa Issuer Privacy Principles are based on the premise that Issuers should recognize and respect the privacy expectations of Visa cardholders.

### **Principle Two: Collect and Use Cardholder Information Only to the Extent Needed**

**Issuers should collect and use information about individual cardholders only to the extent it is needed for their organizations' activities and to provide services and other opportunities to their cardholders.**

Surveys show that one of the principal consumer privacy concerns is the use of information corporations collect. Visa recognizes the importance of this concern. Thus, Issuers should limit the amount of information they collect and use about individual cardholders to what is needed to administer their business activities and to provide services and other opportunities of interest to cardholders.

**Principle Three: Maintain Accurate Information**

**Issuers should have procedures to ensure that cardholder account data -- information directly related to the cardholder's account -- are as accurate, up to date and complete as possible.**

The accuracy of cardholder account data is of particular importance in protecting and maintaining cardholder trust and confidence. The accuracy of cardholder information can also play an important role in the financial and service opportunities available to cardholders. Consequently, Issuers should have procedures to ensure that cardholder account data -- information directly related to the cardholder's account -- are collected and maintained in an accurate, up to date and complete fashion as is possible.

**Principle Four: Maintain Information Security**

**Issuers should maintain appropriate security standards and procedures regarding the unauthorized disclosure of and access to cardholder information.**

A fundamental element of maintaining adequate cardholder privacy procedures is providing reasonable protection against unauthorized disclosure of or access to cardholder information. To properly safeguard cardholder information, Issuers should maintain appropriate security standards and procedures in their business practices and incorporate them into their own privacy policies.

**Principle Five: Limit Employee Access to Information**

**Issuers should implement policies and procedures to limit employee access to cardholder information to a need to know basis.**

Traditionally, business access to cardholder information has been guided by a need-to-know standard: access to such information should be provided only to those employees who have a business need to know the contents. Visa endorses this time-honored standard. Therefore, to help maintain adequate consumer privacy protection, Issuers should implement policies and procedures to limit access to cardholder information to those employees who need to see it in order to carry out the Issuer's business and service functions.

**Principle Six: Restrict Disclosure of Account Information**

Issuers should not reveal specific information about cardholder accounts to non-affiliated third parties, unless (1) the information is provided to help complete the transaction, (2) the cardholder requests it, (3) the disclosure is provided or required by law, or (4) the cardholder has been informed in advance through a cardholder agreement or communication about such disclosure activities.

In addition to the general consumer concern about unwanted uses of their personal information, there is a particular concern among consumers about release of specific information regarding individual financial transactions (such as location and time of purchase and the transaction amount). Visa recognizes the importance of this concern. Consequently, Issuers should restrict disclosure of specific information about individual cardholder accounts to situations where such information is provided to help complete the transaction, when the cardholder requests it, the disclosure is provided or required by law, or where the cardholder has been informed in advance through a cardholder agreement or communication about such disclosure activities. Thus, cardholders might be informed that information about them may be provided to others in connection with various business activities related to their accounts, such as collection efforts, fraud prevention and credit reporting.

**Principle Seven: Honor Cardholder Requests to be Excluded from Marketing Lists**

If an Issuer provides cardholder information to a non-affiliated third parties for marketing purposes, the Issuer shall honor its cardholders' requests to exclude their names from such marketing lists.

According to Lou Harris surveys, most people believe that they do not have control over how information about them is circulated by corporations. Visa recognizes this consumer concern and believes that cardholders should be given an opportunity to request that their information not be made available to non-affiliated third parties for marketing purposes. Therefore, in the event that an Issuer provides cardholder information to non-affiliated third parties for marketing purposes, the Issuer shall honor cardholders' requests to remove their names from these marketing lists.

**Principle Eight: Maintain Cardholder Privacy in Relationships with Third Parties**

**Where an Issuer provides cardholder information to a third party, the Issuer should require the third party to adhere to equivalent privacy standards with respect to that information.**

The significant commitment of Visa Issuers to provide adequate cardholder privacy measures could be compromised if third parties with whom Issuers maintain business relationships do not provide equivalent privacy protections for cardholder information. Consequently, Issuers should require these third parties, when dealing with cardholder information, to adhere to privacy standards that are equivalent to the Issuer's privacy policy.

**Principle Nine: Conduct Employee Education and Monitoring Compliance**

**Each Issuer should educate its employees about its privacy standards and employees' responsibilities to protect cardholder privacy. Issuers should monitor employee compliance.**

Employees of Visa Issuers have a responsibility to help maintain trust and confidence of Visa cardholders and to help to protect the privacy of cardholder information. Accordingly, Issuers should undertake appropriate employee education efforts to help ensure that employees understand the meaning and requirements of their privacy policies. In addition, Issuers should monitor employee compliance with their established privacy policies.

**Principle Ten: Make the Issuer's Privacy Guidelines Available to Cardholders**

**Issuers should make their privacy guidelines available to cardholders.**

An important part of the Visa Issuers' commitment to providing meaningful consumer privacy protection is ensuring that cardholders understand their Issuer's privacy guidelines. Therefore, an Issuer should make its privacy guidelines available to its cardholders to help maintain their trust and confidence.

## BANKING INDUSTRY PRIVACY PRINCIPLES

### **1. Recognition of a Customer's Expectation of Privacy.**

Financial institutions should recognize and respect the privacy expectations of their customers and explain principles of financial privacy to their customers in an appropriate fashion. This could be accomplished, for example, by making available privacy guidelines and/or providing a series of questions and answers about financial privacy to those customers.

### **2. Use, Collection and Retention of Customer Information.**

Financial institutions should collect, retain, and use information about individual customers only where the institution reasonably believes it would be useful (and allowed by law) to administer that organization's business and to provide products, services, and other opportunities to its customers.

### **3. Maintenance of Accurate Information.**

Financial institutions should establish procedures so that a customer's financial information is accurate, current and complete in accordance with reasonable commercial standards. Financial institutions should also respond to requests to correct inaccurate information in a timely manner.

### **4. Limiting Employee Access to Information.**

Financial institutions should limit employee access to personally identifiable information to those with a business reason for knowing such information. Financial institutions should educate their employees so that they will understand the importance of confidentiality and customer privacy. Financial institutions should also take appropriate disciplinary measures to enforce employee privacy responsibilities.

### **5. Protection of Information via Established Security Procedures.**

Financial institutions should maintain appropriate security standards and procedures regarding unauthorized access to customer information.

### **6. Restrictions on the Disclosure of Account Information.**

Financial institutions should not reveal specific information about customer accounts or other personally identifiable data to unaffiliated third parties for their independent use, except for the exchange of information with reputable information reporting agencies to maximize the accuracy and security of such information or in the performance of bona fide corporate due diligence, unless 1) the information is provided to help complete a customer-initiated transaction; 2) the customer requests it; 3) the disclosure is required or allowed by law (e.g., subpoena, investigation of fraudulent activity, etc.); or 4) the customer has been informed about the possibility of disclosure for marketing or similar purposes through a prior communication and is given the opportunity to decline (i.e., "opt out").

### **7. Maintaining Customer Privacy in Business Relationships with Third Parties.**

If personally identifiable customer information is provided to a third party, the financial institutions should insist that the third party adhere to similar privacy principles that provide for keeping such information confidential.

### **8. Disclosure of Privacy Principles to Customers.**

Financial institutions should devise methods of providing a customer with an understanding of their privacy policies. Customers that are concerned about financial privacy will want to know about an institution's treatment of this important issue. Each financial institution should create a method for making available its privacy policies.