GENERAL ISO INFORMATION

1. What name(s) can an ISO use when selling?

* ISO can only solicit using their corporate or DBA name that has been registered and approved with the Associations.
* All additional legal and DBA names must be communicated and approved by MSG Compliance and approved by associations prior to usage

2. What naming convention can a 1099 sales agent use when selling in the marketplace?

* The sales Agent should sell under the registered ISO's Corporate or DBA name
* The Agent may use a DBA name that contains a geographic location or regional sales office only in conjunction with the ISO registered corporate or DBA name.
    1. A Geographic location is defined as a:
        * State
        * City
        * County
        * Region
        * Land Formation
    2. Generalities such as "Metropolitan" are not acceptable without the ISO corporate or DBA name attached
    3. Example of an acceptable Geographic DBA:
        * "ABCISOBostonMetropolitan"
            a. "ABCISO" - This being the Primary ISO name
            b. "BostonMetropolitan" - This being the 1099 Agent name
            c. Note: The naming must be specific to the market they are servicing

3. What does the 1099 Sales Agent need to know about having a website?

* The web URL does not need to be owned by the registered ISO, but can be owned by the 1099 Sales Agent.
* If a 1099 Sales Agent does opt to have their own URL, keep in mind the following:
    1. The contents of the URL must be ISO specific to the registered ISO name.
    2. All solicitations must be performed in the name of the registered ISO.
    3. The URL name may not be referenced within the contents of the website.
    4. ISO Applications posted on these URLs must be branded in the Registered ISO name only.

4. What else should 1099 Sales Agents be aware of when conducting business?

* Telephones:
    1. All phones must be answered in the name of the registered ISO Corporate or DBA name. They cannot be answered in the agent name.
* Email Addresses:
    1. All email inquiries should be addressed to the agent, referencing the registered ISO name. Examples include:
        * "agent"@ ABCISO.com - where the ISO name is "ABCISO"
        * "agent"@ ABCISOBostonMetropolitan.com.
        * Note: Email addresses within these URLS cannot utilize an outside extension, such as "@yahoo.com" or "@hotmail.com" or "@aol.com".
* Non-Merchant Processing Business:
    1. All non-merchant processing solicitations must be segregated from the card processing solicitations.
    2. All Sales Materials must be approved by the Member Bank and FACS and cannot combine merchant processing and non-merchant processing.
    3. URLS - non-merchant processing solicitations must be linked to a separate page, or refer back to the registered ISO, if being contained within the same website.
    4. Rates, fees or Terms and Conditions for merchant processing must not be referenced on pages that also solicit or reference non-merchant processing.

5. As an ISO, what can we do to maintain compliancy with our Sales Reps and Agents?

* MSG recommends instituting some "Best Practices", such as:
* Performing background checks on your Sales Agents
* Providing adequate training and continued education
* Distributing approved collateral and tools to be successful
* Performing periodic checks on Agent websites and marketing materials to ensure continued compliance

6. Can we solicit merchants that are outside the United States?

* Clients may only sign merchant outlets located within the 50 United States and U.S. military bases, U.S. embassies or U.S. consulates located in a foreign territory.
* If an ISO has a relationship with another Acquirer who is conducting business outside of the United States then all websites and sales materials must clearly disclose that this specific Acquirer is conducting the "non US Territory" business.

7. How do we manage our Referral Partners?

* Provide merchants with general benefits but do not quote fees, pricing, terms or conditions.
* Websites must link over to the registered ISO's site to reference terms, conditions, pricing and from a consumer perspective, the consumer must clearly understand and visibly see that they are in a different site/separate link. Telephone referrals must be directed to and serviced by the registered ISO.
* Person to person referral - The Sales Representative must distribute marketing and applications referencing the registered ISO only - again, no pricing quoted or terms and conditions may be discussed.

8. What do we need to know about Community Banks?

* Community Bank must not quote rates, fees, terms or conditions unless registered as an ISO or Affiliate Member Bank.

MARKETING MATERIALS, WEBSITES AND BRANDING

9. What are the steps in developing compliant Marketing Materials and Websites?

* All ISOs should have received a copy of the Merchant Service Group, LLC Services Independent Sales Organization (ISO) Compliance Checklist from their business channel. If you have not received this Checklist, please contact your Relationship Manager/Service Team for a copy. * This checklist is to be used to guide all ISOs when developing/revising any and all Marketing Materials, business cards, mailings or any type of solicitation-related advertisements.
* Please note that this checklist is not to be used as an all-inclusive list, but merely a guide, based on the most common Association requirements.
* Please remember that all marketing materials, websites and all solicitation-related materials must be PRE-APPROVED by FACS and the Member Bank prior to their use and distribution.
* All materials for review and approval should be submitted via Service Center.

10.High Risk/Unacceptable Merchant Types:

* If an ISO has a relationship with another Acquirer that permits solicitation of "High Risk" or unacceptable business - websites and sales materials must clearly disclose the Acquirer that accepts this type of business.

11.Can we use the Merchant Service Group, LLC. logo on our Marketing Materials and Websites?

*Please refer to your Relationship Manager for details on brand and logo usage.

MERCHANT PROCESSING APPLICATIONS AND AGREEMENTS

12.How can we maintain a compliant merchant MPA and Agreement?

* ISO may not make any changes to the MSG LLC Agreement, Application or Disclosure Page.
* All Merchant Applications must be approved by the Member Bank and FACS prior to distribution.
* Applications being used for a specific sales channel within your ISO must not be branded or "stamped" with that Sales Agent's name or market name.

1. Doing so would infer that the sales agent is soliciting under his own name, and hence requiring ISO registration. (Same concept for sales materials)
2. A revised disclosure page now has the "customer service" phone added under the bank phone number.

*ISOs utilizing an online preliminary application must also disclose that a hard copy of the Merchant Processing Agreement and Application (MPA) must be submitted.

PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD

13.What is PCI?

*PCI is the result of the collaborative efforts between Visa and MasterCard to create common industry security requirements for merchants and service providers to proactively protect themselves and the overall payment system against the threat of compromise.

14.What are some important things to remember when it comes to PCI and data security?

* All merchants, Merchant Servicers and third-party service organizations that transmit, store, or process cardholder data for the merchant must be compliant with PCI (Payment Card Industry) standards.
* Merchants must store all material containing account numbers-whether on paper or electronically-in a secure area accessible only to selected personnel.
* Merchants must not disclose cardholder account information to third-parties, except when needed to complete a transaction or when required by law.

* The merchants' disposal procedures must also ensure security; materials containing account information must be made unreadable before they are discarded.
* Merchants must not retain or store Card Verification Value 2 (CVV2) data subsequent to the authorization of a transaction.
* Merchants (and their Merchant Servicers, and third-party service organizations) must not retain full-track magnetic-stripe data subsequent to authorization.
* Merchant contracts with any Merchant Servicer must contain CISP/PCI requirements.

15.Where can we find additional information from the Associations on PCI?

* In 2004, the major brands within the payment industry worked together to create a unified organization called the Payment Card Industry Data Security Standard (PCI DSS) to assist in the management of security. Since then the brands have developed the PCI Security Standards Council, which is an independent organization created to manage the global standards relating to PCI.
* The mission of the PCI Security Standards Council is to:
    1. Develop and maintain global, payment-industry-specific technical data security standards for the protection of account data
    2. Provide a globally available, qualified pool of security solution providers to assist merchants, technology manufacturers and third-party processors in achieving compliance.
    3. Reduce costs and lead times for DSS implementation and compliance by establishing common technical standards for use by all payment brands.
    4. Provide a common and streamlined process for approving Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs), and identifying them through this website.
    5. Provide a collaborative forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of data security standards.
* For additional information regarding the PCI Security Standards Council, please visit www.pcisecuritystandards.org.
* For additional information regarding Visa Cardholder Information Security Program (CISP) compliance validation procedures for merchants and service providers, please visit www.visa.com/CISP.
* For additional information regarding MasterCard Site Data Protection (SDP) compliance validation procedures for merchants and service providers, please visit http://sdp.mastercardintl.com.

16.Are there penalties for working with a merchant or service provider that is not PCI compliant?

* Due to the serious consequences associated with such violations, for any merchant or agent found to have stored magnetic-stripe or CVV2 data, the Acquirer may be subject to the following penalties:

1. A fine of up to $500,000 per violation, per month, until the violation is corrected
2. Compliance actions by Issuers
3. Possible disqualification of the merchant

THIRD PARTY PROCESSORS

17.What is a Third Party?

* Any entity that has access to, stores, downloads or transmits cardholder data.
* Some examples of third parties include (but are not limited to):
* Gateway for transactions from a Merchant location to a Processor
* Provider of Back Office Support (i.e. Customer Servicer, Exception processing for Acquirer's Merchants)
* Supporting loyalty programs
* Electronic Data Capture
* Fraud servicing, monitoring or scrubbing
* Voice authorization and routing
* Call referral processing/telemarketing
* Collections
* Settlement processing
* Cardholder and merchant statement preparation
* Chargeback processing
* Merchant help desk support if there is access to cardholder data
* Loading software into a terminal which will accept cards
* Loading or injecting encryption keys into terminals or PIN pads
* Loading of cryptographic keys into ATMs and cash dispensers
* Deploying and/or servicing qualified ATMs

18.How do the Associations define a Third Party?

Visa USA

Merchant Servicer (MS):

* Merchant contracted relationship
* Not a Member of Visa USA
* Not directly connected to VisaNet

Third Party Processor (TPP):

* Member Bank contracted relationship
* Not a Member of MasterCard International
* Performs transaction and cardholder processing services for one or more MasterCard members

MasterCard International

Data Storage Entity (DSE)

* Merchant contracted relationship
* Not a Member, merchant or MSP
* Stores MasterCard account data on behalf of a member, merchant or MSP.

Third Party Servicer (TPS):

* Member Bank contracted relationship
* Not a Member of Visa USA
* Not directly connected to VisaNet

* Some examples of a Merchant Servicer (MS) / Data Storage Entity (DSE) include (but are not limited to):
* Authorize.net
* Datawire
* Yahoo
* Some examples of a Third Party Servicer (TPS) / Third Party Provider (TPP) include (but are not limited to):
* An Independent Sales Organization (ISO) that conducts their own fraud/risk monitoring or other back office functions.
* When a Member Bank contracts directly with an entity, ex. Credit Discovery or Merlin, to perform fraud monitoring or chargeback processing.

19.How does Merchant Service Group Compliance determine if an entity is a Third Party?

1. Obtain a transaction flow from start to finish to understand:
2. What data is being transmitted, stored or downloaded?
3. How the data is being handled and managed:
    * Truncated vs. Encrypted:
        a. Truncated data may require registration if the data is not truncated according to PCI standards.

b. Encryption requires registration and encryption type should be identified

4. Through what entities does the file containing cardholder data pass through?
5. Review for PCI Compliance Validation
6. Identify the Clearing Member for registration

ENCRYPTION AND SUPPORT ORGANIZATIONS (ESO)

20. What is an ESO?

* An ESO is defined as as any organization, which is not a Plus or Interlink Member, whose Plus / Interlink business relationship with a Plus or Interlink Member involves any of the following activities:

1. Loading software into an ATM or terminal that accepts cards
2. Loading or injecting encryption keys into an ATM or a terminal / PIN pads
3. Providing help-desk support that includes re-programming of ATM / terminal software
4. Generating, storing, or loading / injecting cryptographic keys into PIN pads or ATMs
5. Distributing new DES keys or destroying old DES keys
6. Decommission or commissioning PIN-entry devices
7. Providing general key custodial support services

* Registration and a PIN Security Audit are required. If you use an ESO that performs loading of encryption keys into PIN PADS, please notify your Relationship Manager for further instructions.

ADDITIONAL INFORMATION

Association websites for further information and rules permitted to be distributed to ISOs.

* Visa USA Guidelines for Non Member Agents-Registration, Merchant Agreements, Merchant Acceptance, Merchant Fraud, Risk Management and Risk Control Programs, Cardholder Information Security: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_service_providers.html
* Visa's Payment Application Best Practices:
  WWW.VISA.COM/CISP
* MasterCard Service Provider Rules - MSP Rules, Chargeback rules,Security Rules:
  WWW.MASTERCARDMERCHANT.COM
* MasterCard SDP/PCI:
  HTTPS://SDP.MASTERCARDINTL.COM
* Visa CISP/SDP:
  WWW.VISA.COM/CISP