



ELECTRONIC TRANSACTIONS ASSOCIATION  
*Advancing Payments Technology*

Electronic Transactions Association

# Payment Facilitator Guidelines



October 2016

Authored by



**DOUBLE  
DIAMOND**  
GROUP

for



# Electronic Transactions Association

## Payment Facilitator Guidelines

Payment facilitators (PFs), also known as aggregators, payment service providers or sometimes merchants of record, are growing in number and size around the world. Usually combining payment acceptance with software or other technology, PFs are thought to represent the future of acquiring, especially in emerging markets and verticals. With the explosion of the cloud, there are thousands of independent software vendors (ISVs) emerging, addressing every vertical and geography.

These guidelines were authored by Double Diamond group with input from a working group comprised of risk professionals and other personnel from various ETA member companies. The information contained in this document does not constitute legal advice and should not be relied upon as a substitute for legal advice from counsel.

---

The PF model is designed to make it easier for ISVs to include payments in their offering. Leveraging the PF model, many ISVs are able to combine branding, systems, contracts and servicing between software and payments. They also typically aim to remove friction from their interactions wherever possible. The innovations possible with the PF model tend to attract fast-moving technology companies and startups to the payments arena, which has many positive implications: additional options for the merchant, increased competition, a faster pace of innovation in the marketplace and likely others. At the same time, the new entrants to payments often have little or no experience in payments. As those parties gain access to the payments system, it can introduce new risks.

The payment facilitator guidelines (PF guidelines) provide a framework for how an aspiring PF can properly incorporate risk and compliance practices to reduce risk from the transition into payments. Equally, existing PFs can leverage them to benchmark their current environment and ensure they are meeting industry best practices.

**IMPORTANT NOTE:** While this document is designed to be global in nature, only U.S. law was considered. The recommendations in this document are generally useful worldwide. They should

be considered best practices or building blocks from which a localized set of policies, procedures, processes and practices could be crafted. Generally, most of the guidelines presented herein will be applicable globally, but laws and regulations for any geography outside the U.S. were not considered.

The PF guidelines include tools for the underwriting and risk management of submerchants (also known as sponsored merchants) by payment facilitators as developed by a working group consisting of risk professionals and other personnel from various ETA member companies. These guidelines are not meant as a substitute for any rules or requirements set in place by U.S. laws and regulations, the card schemes, acquiring banks or any other bodies governing the activities of any payment facilitator using these guidelines. Recommendations in these guidelines are not meant to be required in each instance, but they are meant to assist payment facilitators in addressing the risks and concerns identified herein. Each payment facilitator should refer to legal or other counsel for complete guidance. Payment facilitators who provide services to submerchants must understand and follow the rules and requirements for lawful payment aggregation and processing to help avoid harm to consumers and to the payments system.

# TABLE OF CONTENTS

---

<b>1. Introduction to the ETA Payment Facilitator Operational Guidelines</b>	<b>6</b>
1.1. Purpose and Scope of the Payment Facilitator Guidelines .....	6
1.2. Objectives of the Payment Facilitator Guidelines .....	6
1.3. Special Considerations for the Payment Facilitator Guidelines.....	7
1.4. Laws, Regulations and Regulatory Guidelines Considered in these Payment Facilitator Guidelines.....	7
1.5. Organization of These Payment Facilitator Guidelines.....	8
<b>2. Guidelines for Underwriting Submerchant Account</b>	<b>8</b>
2.1. Special Considerations for Underwriting Submerchant Accounts .....	8
2.2. Submerchant Underwriting Best Practice Guidelines .....	9
2.3. Activities That Support Submerchant Underwriting Objectives .....	9
2.4. Submerchant Underwriting Policy Guidelines.....	9
2.4.2. Prohibited Submerchants	
2.4.3. Restricted Submerchants	
2.4.4. Underwriting Risk Levels	
2.4.5. Underwriting Strategies Using Submerchant Risk Levels	
2.4.6. Submerchant Reserves	
2.5. Submerchant Periodic Review .....	13
2.5.1. Periodic Review Effective Tools and Strategies	
2.5.2. Periodic Review of Processing Performance	
2.6. Submerchant Changes.....	15
2.7. Monthly Management Reporting .....	15
<b>3. Submerchants Requiring Enhanced Underwriting Due Diligence</b>	<b>15</b>
3.1. Enhanced Know Your Customer Review.....	15
3.1.1. Know the Principals	
3.1.2. Identify the Business	
3.2. Enhanced Understanding of Internet Submerchants.....	17
3.2.1. E-Commerce Review	
3.2.2. Mobile Commerce, mWebsite and Mobile App Review	
3.3. Enhanced Product Review .....	17
3.3.1. Product Pricing	
3.3.2. Consumer Dissatisfaction Risks	
3.3.3. Potential for Consumer Deceptive Practices	
3.3.4. Membership/Continuity/Multipay Offers	
3.4. Enhanced Review of Certain Marketing Practices.....	18
3.4.1. Negative Option Marketing	
3.4.2. Affiliate/Affiliate Network Marketing	
3.4.3. Telemarketing, including Mail Order/Telephone Order (MOTO)	

3.5. Enhanced Review of Certain Submerchant Types .....	20
3.5.1. Fraudulent Fundraising/Charitable Donation Scams	
3.5.2. Attorney’s Offices	
3.6. Other Guidelines .....	21
<b>4. Guidelines and Objectives for Risk Management of Submerchant Accounts</b>	<b>22</b>
4.1. Special Considerations for Submerchant Risk Management Guidelines.....	22
4.2. Business Goals for Submerchant Risk Management .....	22
4.3. The Objectives of Submerchant Risk Management .....	23
4.4. Activities That Support Submerchant Risk Management Goals .....	23
4.5. Submerchant Risk Management Policy Effective Standards, Tools and Strategies.....	23
4.5.1. Time Frames	
4.5.2. Adverse Actions	
4.5.3. Approval Authority Parameters	
4.5.4. Escalation Requirements	
4.5.5. Documentation Requirements	
4.5.6. Periodic Reporting of Exceptions to Policy	
4.6. Team Communication .....	24
4.7. Effective Tools and Strategies for Daily Exception Monitoring.....	24
4.7.1. The Submerchant Record	
4.7.2. Submerchant Risk Classification Exceptions	
4.7.3. Daily Exception Reports Effective Tools and Strategies	
4.8. Effective Tools and Strategies for Monthly or Periodic Exceptions .....	29
4.8.1. Top Processing Volume, Chargeback Volume, or Refund Volume Report	
4.8.2. Reports by Submerchant Vertical (MCC, Product Type, Agent/Agent Group)	
4.8.3. Restricted Business Type Review Monthly Report	
4.8.4. Monthly Excessive Volume Exceptions	
4.8.5. Submerchants With Decreasing Volume	
4.9. Submerchant Graduation Review .....	30
4.10. Submerchant Changes .....	30
4.11. Monthly Refund Exception Effective Tools and Strategies .....	30
4.11.1. Refund Monthly Exception Thresholds	
4.12. Monthly Chargeback Exception Effective Tools and Strategies.....	31
4.12.1. Chargeback Reporting Threshold Examples	
4.12.2. Chargeback Management Reporting	
4.12.3. Card Scheme Risk Monitoring Program Submerchants	
4.12.4. Chargeback Monitoring and Investigation Procedure Effective Tools and Strategies	
4.12.5. Chargeback Monitoring Team	
4.12.6. Chargeback Activity Monthly Projections	
4.12.7. Chargeback Detail Review Recommendations	

4.13. Effective Tools and Strategies for Investigating Exceptions.....	32
4.13.1. The Purpose of Investigation	
4.13.2. Documenting the Investigation	
4.13.3. Investigation Basics	
4.14. Submerchant Remediation.....	33
4.15. Submerchant Reserves.....	33
4.16. Monthly Management Reporting Effective Tools and Strategies.....	33
<b>5. Risk Management for Submerchants Requiring Enhanced Due Diligence</b>	<b>34</b>
5.1. Enhanced Due Diligence Process.....	34
5.2. Performance Improvement Expectations.....	34
5.3. Reputation Monitoring.....	35
5.4. Secret Shopping.....	35
5.5. Cardholder/Customer Interviews.....	35
5.6. Chargeback Monitoring and Reporting to Card Schemes.....	35
5.7. Enhanced Review of the Sales Processing Method.....	36
5.7.1. Internet Submerchants	
5.7.2. Telemarketing Including Mail Order/Telephone Order (MOTO)	
5.7.3. Mobile Commerce	
5.7.4. Mobile Apps	
5.8. Increased and Expanded Affiliate/Affiliate Network Marketing Review.....	37
<b>6. Requirements for Settlement</b>	<b>37</b>
6.1. Guidance on Financial Operations.....	37
6.2. Graduating Submerchants.....	38
<b>7. Guidance on Transaction Receipt, Authorization Request, Clearing, Chargeback, Representment Records and Billing Descriptor Requirements</b>	<b>39</b>
<b>8. Conclusion</b>	<b>39</b>
Exhibit A: Quick Reference Guide to Applicable Laws and Regulations.....	40
Exhibit B: Website Basic Review Checklist.....	42
Exhibit C: Quick Reference Guide — Online Review Resources.....	43
Exhibit D: Sample Periodic Review.....	44
Exhibit E: 6 Month Trending.....	45
Exhibit F: Quick Reference Guide — Website Meta Tag Review.....	46

# 1. Introduction to the ETA Payment Facilitator Operational Guidelines

## 1.1. Purpose and Scope of the Payment Facilitator Guidelines

The purpose of the ETA payment facilitator guidelines (“PF Guidelines”) is to develop and deliver recommended effective tools to both new and existing payment facilitators. These tools will aid in mitigating risk for members of the Electronic Transaction Association (ETA) as they provide access to practices that have the potential to effectively mitigate payment facilitator (PF) submerchant risk in the U.S. card acceptance ecosystem, depending on the particular situation and the PFs circumstances. A working group consisting of risk professionals and other personnel from various ETA member companies contributed to the development of these PF guidelines.

While at a minimum, PFs are required to follow the rules set in place by card schemes, applicable laws and regulations and their acquiring bank requirements, these PF guidelines provide effective tools for the underwriting, risk monitoring and financial administration associated with the custodial role of funds settlement to submerchants. When used as a guideline for your own underwriting and risk monitoring policies and procedures, these PF guidelines may help eliminate prohibited and undesirable submerchants from entering into or remaining in the card acceptance ecosystem.

Above all, PFs should strive to ensure that they are not providing payment acceptance for submerchants that engage in fraudulent acts or practices that harm consumers and, ultimately, the card acceptance ecosystem. While these PF guidelines serve as a set of tools and strategies that through experience and research have shown to mitigate risk, the transferability of any of these PF guidelines to your organization or their usefulness will depend on your organization’s unique structure, acquiring portfolio composition, and existing practices and processes.

These PF guidelines are intended to provide benchmarks for underwriting and risk monitoring using suggestions made by members of the working group for practices that have consistently shown more favorable results for risk mitigation. While there are many diverse ways to achieve the objectives set forth in these PF guidelines, this document is intended to be agile and evolve as PFs make future contributions and determine better processes for risk management. While not designed

as a standard or requirement for PFs, these PF guidelines can serve as a supplementary basis for self-assessment. PFs may also utilize other reasonable tools and strategies to address the risks and concerns identified to ensure compliance with applicable laws, rules, requirements and regulations.

The U.S. card acceptance ecosystem changes rapidly and requires participants to constantly update and improve upon their policies and procedures. Accordingly, these PF guidelines are a “living” document, which will be reviewed and updated by a select group consisting of risk professionals and other personnel from various ETA member companies. PFs should direct comments or suggestions about these PF guidelines to [Guidelines@electran.org](mailto:Guidelines@electran.org). Recommendations made in this document are intended for U.S. based submerchant oversight.

These PF guidelines do not represent all risk mitigation practices that are being used or that may be used by PFs to effectively manage risk in the U.S. card acceptance ecosystem. Alternative ways to effectively mitigate such risk exist. For example, many PFs likely have and use their own confidential and proprietary practices and processes to effectively mitigate such risk, and such confidential and proprietary practices and processes may not be reflected in this document. Likewise, it is not possible for these PF guidelines to anticipate and answer all questions that may apply to your risk management practices. It is the spirit of these PF guidelines, as well as the documented circumstances within them, that will help PF make sound decisions and define their respective policies and procedures.

## 1.2. Objectives of the Payment Facilitator Guidelines

These PF guidelines identify best practices for underwriting and monitoring along with triggers and thresholds, based on input from the working group, at which PFs may consider flagging prospective submerchants for more in-depth underwriting and existing submerchants for review and potential action. While the thresholds may vary as is determined by individually defined policy, each PF in the card acceptance ecosystem should establish red flags or quantitative thresholds based on varying parameters for the underwriting and monitoring of submerchant accounts. These flags may differ for card present, card-not-present and other submerchant acceptance methods that present various levels of exposure to you or potential consumer harm. These flags and lines will not always dictate action; however, when you have identified a submerchant

for review based on the defined policies and thresholds, you should carefully notate the submerchant's record or file to reflect the factors considered in the review and the basis for making a decision about, or actions taken with respect to, the submerchant as suggested throughout this document.

### 1.3. Special Considerations for the Payment Facilitator Guidelines

Review of a submerchant should take in the totality of circumstances and does not necessarily require application decline or remedial action based on a single issue unless that issue violates a governing standard or your policy. For example, when an item has triggered a PF or a transaction for review, as long as there are not also unacceptable consumer complaints or out-of-market processing statistics for that submerchant, you may decide to take no additional or adverse action and document the submerchant record accordingly. However, if circumstances such as high chargeback or refund rates are combined with severe issues such as identified consumer deception, then it is recommended that you review the submerchant for possible closure.

For PFs that deliver a singularly focused service, either vertically to a specific industry segment or horizontally across a specific technology solution, special consideration or leniencies can be allowed in certain triggers and flags due to the nature of the payment type, actions taken during customer acquisition and known circumstances surrounding the transaction environment. These special considerations should not be applied or weighted if there are other mitigating circumstances identified such as consumer deception or high rates of chargebacks or refunds.

Although the actions taken once a submerchant has been flagged will vary by PF, these PF Guidelines recommend factors and baseline thresholds established by the working group that you should consider. These considerations include determining the point at which a submerchant with circumstances that are difficult or impossible to remediate should be terminated. There are also recommendations for the management of submerchant reserves and determining when it is more appropriate to close a submerchant account rather than mitigate anticipated exposure with reserves or require changes in submerchant practices or other circumstances that led to the issue under review.

It is recognized that there are varying degrees of risks associated with different types of submerchants and processing

volumes. Consequently, it is appropriate to apply varying levels of scrutiny to submerchants based on the individual circumstances. This may range from basic due diligence for the submerchant with an PCI DSS established low-risk profile to a thorough and detailed review for submerchants deemed to present greater risks than established by processing volume alone, such as potential issues with the product itself, how the product is marketed or the delay in the delivery of that product. In addition to requirements for protecting the card acceptance ecosystem and the PF from submerchant fraud and transaction risk, there are regulatory and legal requirements for identification of submerchants and of suspicious activities in order to prevent money laundering and terrorist funding activities. As an example, the USA Patriot Act of 2001 outlines minimum data collection requirements. As such, submerchant identification and know-your-customer (KYC) practices should be a priority in underwriting policies and procedures.

As a best practice, PFs should ensure the delivery of internal and external compliance programs that address:

- Adoption of card scheme reporting requirements for suspicious activity
- Role-based training for underwriting and risk functions to comply with anti-money laundering laws and requirements
- Record retention in accordance with card scheme regulations

This list represents a sample of the regulatory and compliance training necessary to create a PF landscape that minimizes against financial risk and reputation damage. PFs should procure industry expert counsel to ensure their programs adopt necessary card scheme, state and federal guidance.

### 1.4. Laws, Regulations and Regulatory Guidelines Considered in these Payment Facilitator Guidelines

A list of references for laws and regulations considered in the formation of these PF guidelines is included as Exhibit A. PFs should refer to this list as internal practices are being evaluated and developed. This list should not be viewed as an exclusive or comprehensive list of all applicable laws, regulations or guidelines that govern each PF using these PF guidelines, and you should refer to legal or other counsel for complete guidance. It should be noted that local- or state-level regulations have not been considered for purposes of this document.

## 1.5. Organization of These Payment Facilitator Guidelines

The guidelines have been organized to parallel the flow of the risk life cycle of a submerchant – on boarding and underwriting of new submerchants, risk monitoring of live submerchants and periodic reviews based on submerchant performance against certain thresholds and triggers. These guidelines are not meant to address all operational aspects such as 1099-K reporting and record retention requirements or the greater PCI DSS (Payment Card Industry Data Security Standards) requirements.

The underwriting sections of these PF guidelines focus on the how, what and why of submerchant evaluation and underwriting with guidance on special considerations, best practices and areas of compliance. Additionally, activities and standards are included to address small, medium and graduating submerchants. Card scheme prohibited submerchant types are identified as well as guidelines for restricted submerchant best practices.

The section addressing risk management guidelines includes special considerations and business goals as well as effective tools and strategies to mitigate PF financial risk and potential reputation damage. Risk processes and best practices are detailed along with guidance on exception and periodic management reporting. Guidance standards for submerchant risk monitoring practices are detailed in this section, including specifics on the effect of chargebacks on the submerchant risk profile.

To educate PFs on appropriate portfolio oversight, these PF guidelines offer periodic review best practice recommendations relative to the ongoing responsibility of submerchant business performance and evaluation against PF standards. The guidelines offer effective tools, strategies and trending evaluations that are critical to early detection of submerchant risk exposure. Specific thresholds are discussed to provide guidance across a litany of critical business metrics.

## 2. Guidelines for Underwriting Submerchant Accounts

This section is provided as a reference for PFs to use in the submerchant underwriting process to help analyze the risks associated with a prospective submerchant. While PFs are required to comply with card schemes and/or applicable laws and regulations, the recommendations provided may be used to help you evaluate the types and degrees of exposure that different types of submerchants present so that you can develop policies to determine whether risks posed by the submerchant are acceptable or can be mitigated satisfactorily through conditions or restrictions, or whether the submerchant should be declined.

In keeping with overarching goals established by consumer protection laws and regulations that prohibit unfair or deceptive submerchant marketing practices, these PF guidelines for underwriting provide recommendations for greater focus on overall submerchant activity, including data points such as chargebacks and refunds, as well as qualitative factors such as submerchant advertising and marketing methods.

The PF guidelines are not all-inclusive and are presented as a set of examples of effective tools and strategies.

Each PF should establish its own segmented benchmark ratios according to trends identified in the PFs historical processing as demonstrated in Exhibit E that would provoke additional review or enhanced due diligence. For the overarching best practices associated with the metrics suggested in this Section 2, as developed and discussed by the working group, please refer to the Guidelines for Merchant and ISO (Independent Sales Organization) Underwriting and Risk Monitoring January 2016. These guidelines should be reviewed and considered absent more detailed, systematic statistical benchmarking that may be specified in your policy and business plan.

### 2.1. Special Considerations for Underwriting Submerchant Accounts

Certain submerchant types, sales methods or marketing practices may also require additional due diligence or registration as required by the card schemes and regulators. Registration, as well as data security, while not covered in depth in these PF guidelines, should also be a focus of submerchant underwriting as required by the card schemes and as appropriate based on your policies.

PFs that store, transmit or process cardholder data are subject to Payment Card Industry Data Security Standards (PCI DSS) regulations and guidance. Submerchant data security standards and the resulting required actions should be reviewed separate and apart from the PF's own PCI DSS compliance obligations. This document does not opine on PCI compliance. For complete information, please refer to PCICo (Payment Card Industry Data Security Standards Council) and other resources for exact requirements for both the PF and your submerchants.

## 2.2. Submerchant Underwriting Best Practice Guidelines

As a registered PF, it is common to use a frictionless approach to underwriting. However, the PF must take actions that meet legal regulatory and compliance requirements. A minimum set of requirements should:

- Verify the identities and legitimacy of prospective submerchants, the type of business and their owners.
- Check prospective submerchants against the OFAC (Office of Foreign Assets Control) and MATCH (Member Alert to Control High Risk) lists.
- Determine that the submerchant's financial condition is acceptable, as necessary, according to your policy and recommended volume thresholds.
- Determine the extent of risk that the submerchant may pose; for example, possible fraud, credit, financial, compliance, regulatory or reputational risk.
- Ensure the submerchant is in the same jurisdiction as the acquirer

## 2.3. Activities That Support Submerchant Underwriting Objectives

Activities that are recommended in support of your defined submerchant underwriting and business objectives may include the following actions, which are also described in the ETA Guidelines for Merchant and ISO Underwriting and Risk Monitoring.

- Determine that the submerchant and its principals have acceptable credit or bank card processing histories. If utilizing credit reports as part of this process, ensure that practices are in place to ensure compliance with FCRA/FACTA (Fair Credit Reporting Act/Fair and Accurate Credit Transaction Act).
- Determine and confirm what products and services the submerchant is selling.

- Determine and confirm how the submerchant is selling and distributing its products and services.
- Determine if the submerchant's background or method of doing business would preclude the submerchant from being a customer.

For PFs that deliver a singularly focused service, either vertically to a specific industry segment or horizontally across a specific technology solution, special consideration or leniencies can be allowed in certain triggers and flags due to the nature of the payment type, actions taken during customer acquisition or known circumstances surrounding the transaction environment. These special considerations should not be applied or weighted if there are other mitigating circumstances identified such as consumer deception or high rates of chargebacks or refunds.

## 2.4. Submerchant Underwriting Policy Guidelines

Submerchant underwriting policies and procedures should support your business goals, defining expectations for the submerchant underwriting process. Your underwriting policy should have a strong statement of intent that explains your goal for underwriting, including business objectives. Your policy should also include performance objectives that are intended to help you achieve that goal, such as a list of merchant category codes (MCCs) and descriptions of the submerchant industries for which you will (or will not) provide service. Special underwriting considerations that are appropriate based on your established business plan and goals should be noted.

If your business plan includes providing payment acceptance services for submerchants in certain industries, or that are using certain marketing practices to sell products and services to consumers that could present a higher level of risk to consumers and the card acceptance ecosystem, your underwriting policy should describe appropriate due diligence considerations. Focused recommendations for common types of submerchants that fall into this category will be discussed in Section 3: Submerchants Requiring Enhanced Underwriting Due Diligence.

It is recommended to begin with proper and well-documented approval authorities and approval exception processes, which could include those summarized in the following sections. Additionally, PFs should seek legal and oversight reviews to measure practice versus various compliance requirements.

## 2.4.1. Standards for Underwriting

### 2.4.1.1. Time Frames

PFs should establish standards for expected underwriting time frames that are appropriate based on submerchant type, risk classification and individual PF policy. Many PFs offer immediate approval. Such immediate approval will require automated checks as well as more in-depth review once processing begins.

### 2.4.1.2. Approving Authority Parameters

Designated staff approval authority levels for submerchant account approval or parameter changes should include:

- Title and/or position but not an individual's name
- Specify that approval notation is required on the submerchant record

### 2.4.1.3. Identify Third Parties

PFs should know any third parties that are being leveraged by their submerchants during the sales or checkout process. If those or any other third parties have access to credit card numbers, also known as Primary Account Number (PAN) data, the PF should have a process by which they ensure the parties are acting within regulations and properly registered.

### 2.4.1.4. Escalation Requirements

Criteria that could require escalated approval during the underwriting process to a manager or committee such as:

- Request to process larger dollar volume/number of transactions.
- Increased exposure.
- Risk calculated exposure dollar amount exceeds pre-determined authorization levels.
- Restricted MCC codes.
- Restricted submerchant types (e.g., submerchants the PF has defined as higher risk)
- Restricted marketing method(s) employed (e.g., inbound telemarketing, online negative option marketing, etc.).
- Identification of submerchants that are requesting processing levels that require a transition to a direct merchant relationship.

### 2.4.1.5. Documentation Requirements

PFs should have a designated exception notation format as well as a designated review and documentation processes to ensure consistency in underwriting reviews and requirements.

Examples of the items that could be included in the process are:

- The name and title of the person requesting the exception (differentiate between sales representative, underwriter and submerchant).
- The reasons for the exception request.
- The name and title of the person reviewing the request.
- Notation of the exception on the submerchant record with the reason for approval or decline.

It is recommended to use a standardized form for consistency of documentation.

### 2.4.1.6. Periodic Reporting of Exceptions to Policy

Establishment of periodic reporting of all requested exceptions is recommended to be generated on a monthly basis and reviewed in aggregate annually. Examples of items that may be included in this reporting are listed below:

- Requestor name and title.
- Reasons for decline, if applicable.
- Exceptions approved.
- Reviewing/approving individual, name, and title.
- Conditions required for approval.

## 2.4.2. Prohibited Submerchants

PFs recognize that certain types of submerchants carry more risk than others or require specialized expertise to monitor submerchant activity and control risk. Also, certain submerchant types, while accepted as direct merchants, will not be accepted as submerchants as they are prohibited by the card schemes. For these reasons, the PF's policies should clearly outline that the following merchant types will not be considered as submerchants. This list is not meant to be all-inclusive.

All card scheme merchant prohibited types.

- A payment facilitator may not be a submerchant of another payment facilitator.
- Aggregators acting as Payment Facilitators.
- Aggregators acting as Marketplaces (best practice, not required by the Card schemes).
- Illegal business, for example: deviant adult material, counterfeit/trademark infringing merchandise, child pornography.
- Internet pharmacies or pharmacy referral sites (Visa only restriction).

- Outbound telemarketers (Visa only restriction).
- Merchants selling illegal drugs and/or illegal supplements.
- Merchants that violate unfair, deceptive, or abusive acts or practices (UDAAP).
- Merchants who have been terminated. Terminated Merchant File (TMF) or MATCH listing (*Visa only restriction.*)

PFs should recognize that certain types of submerchants carry more risk than others, or require specialized expertise to monitor activity and control risk. Each PF should incorporate a list of prohibited submerchants in its underwriting policy. The policy should also clarify that submerchants of PFs may be declined on a case-by-case basis due to the type of products or business.

#### **2.4.2.1. Minimum Prohibited Submerchant Requirements**

The prohibited submerchant list could contain:

- Card scheme-prohibited submerchants.
- Sponsor bank-prohibited submerchants.
- ISO prohibited submerchants
- Processor-prohibited submerchants.
- PF specific-prohibited submerchants.
- Illegal transactions, determined by jurisdiction.
- This list is not meant to be all inclusive.

#### **2.4.2.2. Prohibited Submerchant Recommendations**

As defined in your business plan, the prohibited submerchant list could also contain:

- Submerchant types
- MCCs
- Sales methods
- Marketing methods that violate UDAAP

#### **2.4.3. Restricted Submerchants**

PFs recognize that business opportunities may be presented by submerchant types that pose increased risks through higher chargebacks and refunds due to the nature of the product or service provided (i.e. items that are easily sold on the black market, items that have little or no value that may be easily disputed, etc.). The risk presented by these business opportunities can be closely monitored and controlled, and therefore mitigated, to present an acceptable level of processing risk.

The PFs policy should clarify that businesses on the restricted

list should be reviewed with greater scrutiny, and the PF should not use frictionless underwriting to board these types of submerchants. Additionally, PFs must adhere to card scheme rules related to registrations and reporting for restricted submerchant types.

##### **2.4.3.1. Minimum Restricted Submerchant Requirements**

PFs should recognize that certain types of submerchants, while carrying more risk than others, may simply require specialized expertise to monitor activity and control risk. PFs should incorporate a list of restricted submerchants in their underwriting policies.

The restricted submerchant list could contain, by way of example:

- Card scheme registerable submerchants
- Sponsor bank restricted submerchants
- PF restricted submerchants

##### **2.4.3.2. Restricted Submerchant Recommendations**

As defined in your business plan, the restricted submerchant list could also include:

- Submerchant type
- MCCs
- Sales methods
- Marketing methods

#### **2.4.4. Underwriting Risk Levels**

Underwriting risk levels should be defined to support an agile approach to underwriting that is adaptable to changing circumstances and constantly reflecting improvement. The underwriting risk levels within policies and procedures should be thoroughly defined based on card scheme and your own individual requirements and risk tolerance as best applied to your business plan or established submerchant portfolio. The policy should be designed to have increasing levels of due diligence, including frictionless if appropriate for your model, as the exposure increases. The recommendations included in these PF guidelines provide examples of such increasing due diligence, which should be adjusted in your policy as best fits your individual goals. All exceptions to defined policies should be well documented within the submerchant record.

Processing risk levels are typically determined by the dollar amount that a submerchant will process or the specific type of exposure, which is typically based on whether or not the card

is present, delayed delivery and other factors the submerchant presents within a stated period.

These PF guidelines recommend a basic, minimum review for all submerchants. Increased processing volumes and exposure risk levels as defined by your policy should require a more in-depth review, as well as higher approval authority levels. These PF guidelines suggest processing level review criteria, which should be adjusted individually by each PF as best fits each category defined by your policy.

#### **2.4.4.1. Defining Underwriting Risk Levels**

Each PF should establish individual definitions for risk levels as appropriate for the defining characteristics of submerchants within the portfolio. Factors that could be taken into consideration when establishing risk levels include:

Submerchant processing volume, card acceptance method and/or risk exposure.

- Micro, mobile and/or small, medium, and large/graduating. Please note that although often found in the micro category, a mobile submerchant may process in any category.
- Higher risk submerchants requiring enhanced due diligence as defined by product type, MCC, prior performance issues. In example, history in card scheme programs such as Visa chargeback monitoring program (VCMP)/excessive chargeback monitoring program (ECP), business risk assessment and mitigation (BRAM) and global brand protection program (GBPP), or other appropriate criteria as well as those submerchants defined as high risk by the card schemes.
- Submerchants who are approved through frictionless onboarding should be further reviewed after the first transaction is processed.

#### **2.4.5. Underwriting Strategies Using Submerchant Risk Levels**

##### **2.4.5.1. Micro, Mobile and Small Submerchants**

When establishing the criteria for this level, it is recommended that you choose a very small processing amount or exposure amount for micro and mobile submerchants based on your risk tolerance. The review below can be automated, with more in-depth review occurring after the first transaction has processed and prior to settlement of that transaction.

Recommended review criteria for this level include:

- A signed application/agreement with all sponsor bank required information. Such agreement is often signed electronically.
- Addresses of both submerchant and principal locations.
- EIN (employer ID number) or SSN (Social Security number) as appropriate.
- American Bank Association (ABA) number, which is the bank routing number, and demand deposit account (DDA) number, which is the checking account number, for the settlement of funds.
- A signed personal guarantee when appropriate.
- Perform a MATCH, or similar, negative file check for each card scheme as appropriate.
- Perform an OFAC and specially designated nationals (SDN) check.
- Authenticate the submerchant through use of third-party resources credit reports, in-house systems or manual review as appropriate for business type based on your policy's definition. At this level, manual review is typically only used when the automated checks are inconclusive or negative.
- Research the entity to verify that the actual business matches the stated business. If the submerchant has a low probability of not processing, this may be chosen to be completed after the first transaction is processed.
- Authenticate the submerchant's location through use of third-party resources, in-house systems or manual review as defined by your policy.
- At a minimum, the website review should ensure card scheme and individual PF prohibitions do not exist prior to processing, and complete a full website review should be undertaken once processing has begun. A sample website checklist has been provided as Exhibit B.

##### **2.4.5.2. Medium Submerchants**

When establishing the criteria for this level, you should choose a medium processing amount or exposure as well as appropriate average ticket size for medium-sized submerchants based on your risk tolerance.

It is further recommended that if chargebacks are above 0.30% or a number defined by your policy (determined statistically significant), or credits are not appropriate for the industry, obtain the information required for large submerchant processing.

Recommended review criteria for this level include:

- All items in micro, mobile and small submerchant process should be reviewed.
- Conduct a review of credit history, and set a minimum condition below which the submerchant will be declined.
- Complete review of website as required by the card schemes, if not previously completed.
- Perform a review of the submerchant location (can be virtual review) as appropriate for the submerchant type, defined in your policy.
- Gain a better understanding of the submerchant business and marketing methods.
- Review online reputation tools such as social media, complaint forums and public action notices from sources such as those listed in Exhibit C.
- Obtain the business license or equivalent.

#### **2.4.5.3. Large/Graduating Submerchants**

- When establishing the criteria for graduating submerchants, PFs must adhere to card scheme thresholds for processing volumes of the submerchants. Card scheme limits for submerchant processing is stipulated as follows:
  - If the submerchant has more than \$100,000 in Visa volume in a calendar year, the submerchant must enter into a direct merchant relationship. The funding flow does not have to change.
  - If the submerchant has more than \$1,000,000 in MC volume in a calendar year, the submerchant must enter into a direct merchant relationship and receive direct funding/settlement from the bank.

The PF is responsible for monitoring the volume thresholds and adhering to the card scheme volume mandates. Failure to do so could result in program fees and fines.

Once the submerchant has graduated, please refer to the Guidelines for Merchant and ISO Underwriting and Risk Monitoring published January 2016 for the detailed overview of underwriting best practices.

#### **2.4.5.4. Restricted Submerchants**

Submerchants that have been designated as restricted submerchants based on your policy should be reviewed with the criteria one level greater than the submerchant's requested processing level. Restricted submerchants should not be approved using a frictionless method and should always be manually reviewed using the additional due diligence recommendations for higher risk submerchants that are further detailed in Section 3 as appropriate based on the submer-

chant's business type.

#### **2.4.6. Submerchant Reserves**

Reserves are not typically applied to submerchants. However, if the PF decides reserves are necessary, please refer to the Guidelines for Merchant and ISO Underwriting and Risk Monitoring published January 2016 for the detailed overview of reserves. As included in the referenced January 2016 guidelines, personal/corporate guarantees might be an alternative to reserves.

Reserves should not be used as a way to accept submerchants engaging in acts or practices that are unfair, deceptive or abusive to consumers. In lieu of accepting the submerchant with a reserve, these submerchants should be denied the ability to process.

Reserves should not be used as a mitigation tool in order to accept a submerchant when card scheme or regulatory fines are expected. Unless mitigating factors exist that are approved by your senior management and documented on the submerchant record, that submerchant should be declined during the underwriting process or closed if currently processing.

#### **2.5. Submerchant Periodic Review**

Each PFs underwriting policy should contain a section that defines the types of submerchants that should be subject to periodic review (e.g., graduating submerchants as defined by card scheme requirements or submerchants that otherwise pose increased levels of exposure, whether monetary, reputational or regulatory) to your portfolio. The underwriting policy should also specify when and how submerchants will be reviewed on a periodic basis. The policy should define periodic review timeframes for submerchants based on dollar volume and number of transactions processed or exposure over a specific time frame. When performing the periodic review, each PF should obtain updated documents commensurate with the submerchant's processing level and overall risk exposure.

##### **2.5.1. Periodic Review Effective Tools and Strategies**

Each PFs policy should at minimum reflect annual review requirements established by the card schemes and is recommended to include the following:

- Financial information (or updated financials) when appropriate and in correlation to the processing volume or risk exposure of the submerchant. While this is not a typical requirement for a nongraduated submerchant, such documents may be requested during a review.

- Ensure no changes have been made to the approved sales method or product; likewise, you may want to validate that the submerchant MCC continues to reflect the submerchant principal business activity.
- Follow approval criteria set forth in the appropriate section of the underwriting policy.
- Reputation reviews of the business and principals should be completed, which may include online research using tools listed in Exhibit C.
- You should use a standard form to ensure consistency. (Exhibit D has been provided as an example.)
- You should review current processing, as applicable, to ensure submerchant is in good standing. (Exhibit E has been provided as an example.)
- You should ensure graduating submerchants migrate to direct merchant status at their mandated volumes.

### 2.5.2. Periodic Review of Processing Performance

Each PF should indicate in its policy performance thresholds at which submerchants should be flagged for review or assigned to an increased risk level. It is advisable to identify a submerchant trending with issues prior to that submerchant reaching the card scheme defined violation thresholds. An example of trend reporting has been provided in Exhibit E.

The specific ratios provided in the subsection below are examples.

#### 2.5.2.1. Six-Month Trending Review

A six-month trending report should be generated, including the transaction numbers and dollars for sales, chargebacks and refunds, as well as any other information you deem pertinent to the performance of the submerchant.

- Sales should be consistent, similar from month to month or show appropriate growth with no spikes unless seasonal or documented as approved on the submerchant record.
- You should investigate a spike or drop in sales.
- Rolling spikes and drops should be carefully reviewed.

#### 2.5.2.2. Six-Month Chargeback Activity Review

The last six months' chargeback activity should be broken out by month to compare performance month to month. Each PF should define thresholds requiring escalated review or action taken based on ratios of chargeback count and amount

compared to transactions processed each month. In addition to reviewing dollar/count ratios and thresholds, a PF should also review chargeback reason codes to ensure the deceptive practices/fraud reasons are within acceptable limits for the submerchant category. Examples of ratios of the number of chargebacks to the number of sales that could require escalated review are:

- While it is ideal for a submerchant to have a ratio (number of chargebacks divided by number of sales for a specific month) less than 30 basis points (BPS), a submerchant with a ratio of greater than 70 BPS is a higher risk submerchant and should require enhanced due diligence.
- If total number of chargebacks is below 25, a higher ratio may not be as alarming but should be investigated when above 2.5%.
- You should review any related submerchants (same ownership as an example) that when assessed cumulatively might result in violation of your policy.
- Gamer sites, digital goods, online clothing sales and entertainment may have chargeback ratios that are higher than other submerchant types; therefore, acceptable levels should be determined by MCC within your policy.

#### 2.5.2.3. Six-Month Refund Activity Review

The last six months' refund history should be broken out by month to compare performance month to month. Each PF should define thresholds requiring escalated review or action taken based on ratios of refund count (number of refunds divided by number of sales in a month) and amount (\$ of refunds divided by \$ of sales in a month) compared to transactions processed each month. Examples of ratios of the number of refunds to the number of sales that could require escalated review are:

- For card not present or future delivery a refund ratio of less than 5% and/or greater than 10%, may require increased review. The typical refund range for a higher due diligence submerchant is generally between 5 and 10%.
- Digital goods typically have a refund ratio closer to 10%.
- Card present should be less than 4%.
- Credits on special order products, even one or two, may be an indicator of product issues.

## 2.6. Submerchant Changes

Changes to account information, ownership or organizational structure for submerchants should be reviewed to ensure changes are made in accordance with your policy, do not present additional risk exposure beyond what is acceptable to you, and do not require additional due diligence or have card scheme registration requirements.

Each PF policy should outline submerchant changes that may pose additional risk and contain procedures to be followed.

Examples of changes that may prompt review include:

- Submerchant DBA (doing business as) changes, especially in the first three months of processing.
- Ownership changes.
- Legal or tax ID changes.
- Any descriptor changes.
- Changes to business type or product offerings.
- Any phone number changes.
- Website changes.
- DDA changes.
- Address changes.
- Multiple address changes within a short period of time.
- MCC changes.

Reviews may be prompted by single, multiple or combined instances within assigned time frames as defined by your policy.

## 2.7. Monthly Management Reporting

The establishment of monthly management reporting is important to ensure that there is appropriate senior level oversight of the day-to-day activities within the underwriting department. Monthly reporting should provide a high-level summary regarding activity deemed to warrant management or senior-level attention, as based on each PFs individual policy. PFs with large submerchant portfolios may wish to create separate levels of reporting requirements for respective management levels.

Each PF will determine what types of reporting are appropriate for individual use.

## 3. Submerchants Requiring Enhanced Underwriting Due Diligence

Certain types of submerchants require enhanced due diligence in addition to the strategies previously outlined for general submerchant underwriting and in addition to the minimum requirements established by applicable laws, regulations and card schemes. Sponsoring these types of submerchants often comes with additional due diligence requirements, monitoring and staffing responsibilities regardless of the processing level.

PFs often attract business segments such as charities and attorney's offices as submerchant types, which are some of the business types that represent a category recommended for incremental review with enhanced due diligence. The ETA Guidelines for Merchant and ISO Underwriting and Risk Monitoring should be referenced by the PF for a broader scope of review on other higher risk merchant types recommended for enhanced due diligence to avoid reputation, regulatory and credit and other risks.

Higher risk submerchants are labor intensive, often requiring manual oversight by staff. Some higher risk submerchant types have additional mandatory registration requirements with the card schemes. (Please note that registration is outside the scope of this document. To determine all circumstances when a submerchant should be registered with the card schemes, please refer to the card scheme rules.)

In all cases where a higher risk submerchant is considered for approval, direct conversation with the submerchant is an effective strategy when performing the additional due diligence recommended in this section. The recommendations included in this section, which define steps for specific submerchant categories, are not necessarily exhaustive. Sponsoring higher risk submerchants requires case-by-case assessments of risk. Thus, some of the steps identified below may be unnecessary in the context of a particular submerchant relationship. At other times, those steps should be augmented by additional measures to protect against reputational risk and injury to consumers, as well as increased risk monitoring during the submerchant relationship.

### 3.1. Enhanced Know Your Customer Review

#### 3.1.1. Know the Principals

##### 3.1.1.1. Owner/Principal Information

Ensure the submerchant owner information (location, income, experience and other demographics) makes sense according to the submerchant and industry type.

### 3.1.1.2. Background Checks

Background checks should be completed for owners of higher volume submerchants or when ambiguous information is found.

A legal review should be completed for high-risk accounts that could include the following:

- Lawsuits the submerchant has filed as well as lawsuits that have been filed against the submerchant or its principals.
- Federal or state law enforcement actions initiated against the submerchant or its principals (including, without limitation, Federal Trade Commission or state attorney general actions).
- Complaint records filed with the Better Business Bureau, online complaint boards and other such complaint repositories.
- Social media and other online reputation investigation should be used as a tool for research.
- Understand the circumstances outlined in all blogs and complaints.
- Review positive information as well to ensure the source of any negative information appears reputable and not an attempt to discredit the submerchant.
- Perform public records searches.

### 3.1.1.3. Interrelated Companies and Beneficial Owners

Additional care should be taken to monitor for attempts to conceal interrelated companies or the true owners of a submerchant for purposes of evading card scheme rules or other regulatory considerations.

An entity may, for example, attempt to open multiple submerchant accounts in the name of different but related submerchants in order to avoid regulatory scrutiny. Reasonable due diligence should be conducted to screen for indicia of corporate relatedness such as:

- Request information on related submerchants, companies, principals and beneficial owners.
- Check business and individual information (e.g., names, addresses, customer service numbers, contact numbers and email address) against those of other submerchant accounts to identify related entities.
- Multiple websites with identical verbiage, look and feel.

Similarly, a submerchant may seek to set up companies with listed principals (e.g., family members or employees) that camouflage the real people (known as beneficial owners) who own, control and profit from the submerchant account. This may be done for purposes of diluting volumes to avoid

detection in card scheme chargeback programs or hiding beneficial owners who may have been previously listed on MATCH or are under current scrutiny by regulatory or law enforcement agencies. When using online tools to search for linking information, including the presence of beneficial owners, some questions you could ask are listed below:

Does the submerchant have any beneficial owners not listed in the application materials?

- If yes, obtain additional information on the listed principals and the beneficial owners, such as:
  - Are they related?
    - Do they live in the same area?
    - Do they belong to similar organizations or attend the same school?
    - Are they linked on social websites such as Facebook or LinkedIn?

Perform searches on:

- Customer service numbers
- Contact phone number
- Cell phone number
- Fax number that is sending the application if hard copy
- Contact person name
- All owner names and business names
- Addresses (business and personal)
- Email address and domain of email if unique (i.e., not Yahoo, etc.)
- IP addresses, footprint, device ID
- Descriptors

## 3.1.2. Identify the Business

### 3.1.2.1. Ensure the Legitimacy of the Business

- Search all phone numbers online.
- Check if affiliated with other businesses.
- A physical site survey should be conducted on high-risk submerchants.
- If social media and other online research tools are used in lieu of the physical site survey, the submerchant record should be well documented.
- Online mapping (e.g., Google Maps) or satellite views should clearly show the business.
- <http://www.blackbookonline.info/> or other online resources can be used for further research.

- An appropriate site survey or business verification should be conducted on third-party vendors performing critical operational services for the submerchant, including but not limited to:
  - Fulfillment houses
  - Sales call centers
  - Customer service call centers

## 3.2. Enhanced Understanding of Internet Submerchants

### 3.2.1. E-Commerce Review

A website review checklist has been included as Exhibit B.

- General website review:
  - Goods and services should be consistent with submerchant application. It is recommended that PFs use a third party to review submerchant websites for potential counterfeit/IP infringement.
  - Business address and phone number should match the application.
  - Currency should be in U.S. dollars.
  - All URLs associated with the business should be reviewed.
  - The country of record should be listed.
  - Card scheme logos should be properly displayed.
- Billing terms:
  - You should review for negative option marketing.
  - You should ensure that the billing terms are accurately and completely displayed in a clear and conspicuous manner before consumers confirm the purchase.
  - There should be no pre-checked products or services.
  - All products and services billing terms should be explicitly agreed to by the consumer (e.g., nothing should be hidden in inconspicuous fine print).
  - Checkbox/acceptance of offer terms and conditions should not be pre-checked.
  - You should review for secure checkout page.
  - Delivery method.
  - You should require notification of material changes and monitor delivery times on larger submerchants through methods such as secret shopping (discussed in Section 5.4).
- Cancellation/Return/Refund Policies:
  - You should ensure cancellation, return and refund policies are clearly explained.

- You should ensure business names and contact information listed match the application information.
- Customer service/contact information should be clearly and conspicuously displayed.
- You should verify that phone numbers are in service and answered appropriately.
- The representative should answer in a timely manner.
- The business identified should be the appropriate business.
- You should look for hidden Web page content that may indicate the website is used for another purpose than indicated.
- You should review all links for compliance with underwriting guidelines.
- You should examine empty space for hidden links/content (hover the mouse over empty spaces).
- You should review meta tags as shown in Exhibit F.
- You should review website Who-Is or similar registration and Alexa data.
- Non-U.S. registrations should require increased scrutiny or due diligence. It is a recommended practice to require the submerchant to publicize nonpublic website registration information.

### 3.2.2. Mobile Commerce, mWebsite and Mobile App Review

Regardless of the screen size or character limitations, mobile websites and mobile apps should be reviewed under the same principles as nonmobile website, described above, as all requirements for clearly explaining offer and billing terms are the same. The submerchants should account for screen size or other limitations when presenting offer terms or other disclosures.

When reviewing mobile sites and apps, ensure they are consistent with the non-mobile sites.

## 3.3. Enhanced Product Review

The product being sold is a key component when reviewing the submerchant. Priority should be given to making sure that submerchants are truthfully explaining the product. All submerchants should adhere to laws prohibiting unfair, deceptive, or abusive acts or practices (UDAAP) when describing the products they sell. Some products have stricter regulation than others, requiring adherence to laws such as the Telemarketing Sales Rule, the Mail or Telephone Order Merchandise Trade Regulation Rule, and the Restore Online Shopper's

Confidence Act. In addition, certain product types also have rules governing how they are marketed, including the Business Opportunity Rule. These rules, along with their links, are listed in Exhibit A.

### 3.3.1. Product Pricing

The product pricing should be in line with the reasonable value of the product based on a review of competitor offerings (e.g., a Gucci purse offered for sale for \$100 is clearly incorrect and may indicate fraud or counterfeit goods). Claims of “free” should truly be free with no hidden shipping charges or other fees, in accordance with the Federal Trade Commission’s guide concerning use of the word “free” and similar terms. Savings claims should be legitimate, substantiated and realized by the consumer in a reasonable time frame.

### 3.3.2. Consumer Dissatisfaction Risks

- The marketing should “make sense” for the intended target consumer.
- It should be determined whether the product type inherently has a higher risk of consumer dissatisfaction.
- Online searches of the business, all principals and product names should be initially and continually performed.
- Searches should include review for negative publicity.
- Searches should include keywords such as “scam” or “sucks.”

### 3.3.3. Potential for Consumer Deceptive Practices

Each PF should review product and service offerings to assess the potential risk of unfair, deceptive, or abusive acts and practices defined unlawful by the FTC and UDAAP laws and should engage legal counsel as needed to assess these potential risks.

### 3.3.4. Membership/Continuity/Multipay Offers

- Each PF should ensure the terms of the sale are clearly defined.
- Cross sells should be clearly identified and presented concurrently with the original sale.
- Upsells presented after the primary offer is accepted should be clearly identified and require direct consumer action to purchase.
- All cross sells and upsells should be separately agreed to by the cardholder.

## 3.4. Enhanced Review of Certain Marketing Practices

Marketing is a key component to the understanding a consumer has of the product or service the submerchant presented for purchase. Priority should be given to making sure that submerchants are not using sales tactics that could be considered unfair, deceptive, or abusive acts and practices. All submerchants should adhere to UDAAP laws and regulatory guidance from consumer protection agencies. Some types of marketing have stricter regulations than others, requiring adherence to laws such as the Telemarketing Sales Rule (telephone sales), the Mail or Telephone Order Merchandise Trade Regulation Rule (mail, telephone and Internet sales), and the Restore Online Shopper’s Confidence Act (Internet sales).

You should identify how the submerchant markets. If the product type or submerchant type necessitates (i.e., the product or submerchant poses a higher risk due to the processing methods or product type), you may seek an attestation or legal opinion letter stating that the submerchant is following applicable laws, or have an attorney review the submerchant’s practices. However, if you obtain an attestation or legal opinion from the submerchant, it should not be used in lieu of the proper diligence described throughout this document and more specifically identified in this section.

Some examples of submerchant types that may merit attestation include, but are not limited to:

- Gambling and fantasy sports
- Tobacco sales
- Pharmaceutical sales (if allowing for MasterCard only, prohibited Visa)
- Nutraceutical sales
- Payday lending or other money service types of businesses such as car title loans or money transfer
- Multi-Level Marketing businesses

### 3.4.1. Negative Option Marketing

The PFs underwriting policy should address when it is acceptable to approve a submerchant using negative option marketing. Negative option marketing includes any marketing where the consumer’s silence or failure to affirmatively act is treated by the submerchant as acceptance of an offer. Common types of negative option marketing include free trial offers, continuity programs and subscription plans.

Submerchants that use this marketing method pose a greater risk of harm to the consumer and, therefore, the card acceptance ecosystem. As a result, they should be scrutinized more diligently during the underwriting process. Each PF should consider the following recommended practices if accepting submerchants using negative option marketing:

Free or low-cost trials should be a minimum number of days.

- The minimum number should be long enough to allow for the product to be shipped and used.
- By way of example, 10 days is recommended as a minimum trial for digital goods; 14 days is recommended as a minimum for tangible goods.
- Should begin after the product has been shipped.
- Shipping and handling should not be billed as a separate transaction from the product/service.
- Low-cost trial periods with deferred billing and/or shipping-only costs pose a higher risk and should be closely monitored.
- All material terms and conditions of the offer must be disclosed in a clear and conspicuous manner, adjacent to the order submit button. “Clear and conspicuous” means that the offer disclosures are unavoidably noticeable, in a typeface and font size easy to see and read, and written in language that is easy for the consumer to understand.
- Material terms and conditions include, without limitation, the fact that the consumer must take some affirmative action, such as calling customer service to cancel, to avoid future charges; the costs and frequency of any future recurring shipments, including shipping and handling (if applicable); whether the consumer must return product to avoid further charges, including whether the consumer must obtain a return merchandise authorization (RMA) number and pay for return shipping costs; and, as applicable, the number of shipments the consumer is required to receive, or the fact that the consumer can call to cancel further shipments at any time.
- The submerchant must obtain the consumer’s affirmative consent to the offer terms and conditions. Using a checkbox to indicate agreement to the clearly disclosed offer terms is preferred, but clearly labeled order acceptance instructions may be suitable depending on the circumstances. If a checkbox is used, it should never be pre-checked.
- Opt-in options for additional products or enrollment in continuity should not have a pre-filled checkbox.
- Any marketing or claims that could be considered deceptive, exaggerated or unsupported should not be permitted. Legal counsel should be consulted when determining whether marketing or claims qualify as

deceptive, exaggerated or unsupported. A nonexhaustive list of examples is below.

- Too-good-to-be-true product.
  - Unreasonable guarantees.
  - Celebrity endorsements (should have proof of endorsement).
  - False sense of urgency.
  - Fake blogs or articles – news stories. (It is an effective strategy to search the name of a periodical or a news media entity mentioned to ensure it is real.)
  - Testimonials (should have proof of occurrence).
  - Health claims (should have substantiation such as clinical trials).
- A third-party vendor should be used to provide substantiation if the product is a pharmaceutical or nutraceutical.
  - Cannot not allow third-party data pass.
  - Should ensure the descriptor is easy to understand from the cardholder’s vantage point.

PFs should recommend that submerchants use technology such as gateways or customer relationship management software (CRMs) that allow for merchant-defined fields to be assigned to the transaction to provide more data to assess performance of specific offers, affiliates or other marketers. A nonexhaustive list of suggestions is below.

- Assign (stock keeping unit) SKUs to specific product offers.
- Track phone numbers to gauge sales/customer service performance.
- Track source websites generating traffic.

### 3.4.2. Affiliate/Affiliate Network Marketing

Affiliate marketing is a commonly used type of performance-based marketing for Internet submerchants. In this model, merchants pay “affiliates” (also referred to as “publishers”) for website traffic or sales generated by the affiliate’s own marketing efforts. Some merchants contract directly with individual affiliates, while others contract with “affiliate networks” that manage groups of affiliates working within the network. In the latter model, affiliate networks are responsible for compensating the individual affiliates.

These PF guidelines contemplate that affiliates processing volumes typically qualify these MCCs as direct merchants. Please refer to the Guidelines for Merchant and ISO Underwriting and Risk Monitoring published January 2016 for the detailed overview of the use of affiliates.

### 3.4.3. Telemarketing, including Mail Order/ Telephone Order (MOTO)

For submerchants engaged in sales via telemarketing, you should review the submerchant's policies and procedures for compliance with the Telemarketing Sales Rule (TSR), the Telephone Consumer Protection Act (TCPA) and other applicable laws and regulations. Please note that Visa does now allow outbound telemarketing merchants to be submerchants in a PF.

The following guidelines or other reasonable strategies identified by the PF to address telemarketing and MOTO risks are recommended when underwriting any submerchant engaged in telemarketing:

- You should review and understand all scripts to be used.
- You should review and understand all upsell scripts, if applicable.
- You should review whether the submerchant uses third-party verification of sales (by a person other than the sales representative).
- It is an effective tool for the verifier to ask if the sales agent promised anything to the consumer that was not spoken of during the verification call.
- You should be aware of specific requirements in the TSR or the TCPA applicable to certain types of submerchants (e.g., submerchants engaged in sales of debt relief products or services).
- Submerchants that make outbound calls of any type – direct dial or via a prerecorded voice message (i.e., robo-calling”) are not allowed by Visa to participate in the card acceptance environment as a submerchant. These types of businesses are eligible only as direct merchants.
- You should understand the specific payment methods that the submerchant will use to accept payment from consumers. The TSR prohibits submerchants from accepting remotely created checks (RCCs), remotely created payment orders (RCPOs), cash-to-cash money transfers and cash reload mechanisms for telemarketing sales.

It is a recommended practice to know and confirm the identities and reputation of third-party vendors providing services integral to the submerchant's telemarketing business such as:

- Customer service
- Fulfillment houses
- Return processing

### 3.5. Enhanced Review of Certain Submerchant Types

Certain types of submerchants pose a higher risk of harm to consumers if sales, marketing, fulfillment, customer service and other business practices are not conducted by the submerchant in compliance with laws, regulations and legal guidance issued by regulators. While categorical exclusions of submerchant types from the payments industry are not mandated, the following submerchant types may require further evaluation before becoming a submerchant.

Please refer to the ETA Guidelines for Merchant and ISO Underwriting and Risk Monitoring, January 2016 for information on increased diligence for the merchant types listed below.

Examples include:

- Short-term, dollar consumer lending/payday lending
- Debt collection
- Debt relief services
- Money-making opportunities/work-from-home/coaching and mentoring
- Business opportunities and multilevel marketing

#### 3.5.1. Fraudulent Fundraising/Charitable Donation Scams

Charitable organizations are often set up for specific events or require special, targeted software. It is these characteristics that make them suited to be submerchants. Unfortunately, many scams pose as charitable organizations. Because of this, the PF must take extra care when underwriting them.

- A 501c(3) or applicable government document must always be obtained, reviewed and understood.
- While 8398 is most often the correct MCC, other MCCs that are often assigned for these submerchants are 7299, 8399, and 8999.
- Fraudulent charitable fundraising often involves for-profit companies that make misrepresentations about charitable donations, including but not limited to, the following practices:
  - Misrepresentations about the identity of the solicitor.
  - Misrepresentations that donations will be used to benefit particular organizations, programs or causes.
  - False claims that contributions will be used locally or to support causes appealing to consumers.
- The terms of service agreements between for-profit fund-

raisers and charitable organizations may also be unfair or deceptive. One example is an agreement where the service provider keeps the majority of donations collected for its services and gives very little of the collected donations to the charitable organization. These arrangements are usually unknown to consumers, who believe all or most of their funds will benefit the charity.

- PFs providing processing services to for-profit fundraisers, or charitable organizations that contract with for-profit fundraisers, should review the business arrangements of these relationships, consumer complaints and other information sources to identify these practices.
- Also consider whether evidence in an underwriting file and related background checks for a nonprofit submerchant may suggest that the nonprofit entity has been set up to hide unlawful or criminal activity, facilitate money laundering, or move money out of the country.

### 3.5.2. Attorney's Offices

Many attorney offices are structured in a manner that lends themselves to submerchant processing relationships. When working with attorney offices, a PF should understand the relationship between the lawyer and the firm, the types of clients represented and the types of receivables that will be payable by credit card. Best practices include evaluating the attorney's client satisfaction policy to ensure how discrepancies in services received will be handled. Special diligence should be given the following payment characteristics:

- Collection of normal and customary fees and pass-through expenses.
- Retainer values should be in alignment with potential settlement or case values.
- No collection/disbursement of legal settlements via credit card.
- No payment of amounts previously written off by any party.

### 3.6. Other Guidelines

There are other effective tools and strategies that do not fit into the categories listed above however, they should be followed. They are included below in no particular order.

- You should know discounts and other fees charged and should ensure consistency with industry/type.
- Out-of-market fees charged to and accepted by a submerchant may be an indicator of a high-risk submerchant and should be investigated.

- Submerchants operating in known high-risk areas such as Utah; Las Vegas, Nevada; Brooklyn, New York; Dade and Broward Counties, Florida; and others that may be identified by the PF should be reviewed with greater due diligence.
- You should monitor law enforcement activity and industry publications for trends and patterns in higher risk submerchant activity. Examples include but are not limited to:
  - FTC press releases (individuals and business entities).
  - CFPB press releases (individuals and business entities).
  - MAC (Merchant Acquirers Committee) alerts (individuals and business entities).
  - Attorney general cases.
  - Better Business Bureau alerts.
  - News alerts and feeds.

The PF should maintain an internal negative database (sources outside of MATCH or other card scheme-maintained negative databases) that may be searched by many different fields.

## 4. Guidelines and Objectives for Risk Management of Submerchant Accounts

While PFs are only required to comply with card schemes and applicable laws and regulations, proper management of a submerchant portfolio necessitates a strong focus on identifying and mitigating submerchant activities deemed to pose risks and determining the nature and extent of the exposure that a risk presents. This section should be used in the risk management of submerchant portfolios. For additional guidance, PFs may reference the ETA Guidelines on Merchant and ISO Underwriting and Risk Monitoring, January 2016.

Traditionally the monitoring of daily processing statistics and chargeback activity has been accepted within the processing industry as the primary identification method for potential submerchant fraud or unsatisfactory account performance. In addition, there is now a heightened regulatory focus on refunds issued as an additional measure of submerchant performance and, consequently, consumer satisfaction. PF systems should require that refunds be linked to an original sale.

Internal and external resources should provide reports on a daily basis that identify potential risks and fraud. In order to maintain a viable processing relationship, submerchants should be questioned regarding exceptions to normal or expected transaction activity.

The parameters provided in this section are not all inclusive and are presented as examples meant to serve as an indication of when submerchant activity is recommended to be flagged for review by the PF. Flags for specified activity do not inherently mean that the submerchant or the flagged event is bad or that the actions listed should be taken on the account. Flags simply indicate that the identified activity is outside of the approved or typical parameters for the submerchant or otherwise indicate there is potential for a larger issue. Flags are typically investigated by risk analysts for resolution.

### 4.1. Special Considerations for Submerchant Risk Management Guidelines

It is particularly important to view submerchant performance holistically and not focus on single exceptions. While you may be comfortable with one exception occurrence for a submerchant, when that isolated event is viewed along with all other exception occurrences, higher risk marketing methods, negative indicators from Internet research, or other activity recommended to be reviewed, the totality of the submerchant circumstances may be viewed with greater concern

or warrant an escalated course of action. The goal of this section is to provide effective tools to help you understand the submerchant in its entirety. As with the underwriting of submerchant accounts, it is likewise important to establish an agile approach to risk management. As new fraud trends and high-risk activity related to credit card processing are identified across the industry, your policies and procedures, exception criteria, and periodic monitoring should be evaluated and adjusted accordingly as appropriate based on your business plan and established risk tolerances.

At all times, risk analysts should use their best judgment as it relates to the specific submerchants and business types. The analysts may request additional information or impose restrictions (e.g., processing caps, delayed funding, lower chargeback or refund ratio thresholds) if necessary for reasons including but not limited to transaction processing activity (including daily processing, refunds and dispute activity), changes to owner credit or business financial condition, changes to the business model or to the accepted risk level of the business model, or other combinations of factors.

However, if activity is flagged, and there are also unacceptable levels of consumer complaints, then higher due diligence and potentially adverse action are more likely to be appropriate. If processing activity reaches a level of greater concern, and investigation reveals that the submerchant is engaging in practices that could be considered unfair, deceptive or abusive to consumers, that submerchant should be terminated. In those cases, the availability of mitigating actions such as establishing a reserve should not dissuade any PF from terminating the submerchant. PFs should comply with UDAAP requirements, which address many of these topics.

### 4.2. Business Goals for Submerchant Risk Management

Each PFs risk management policy should have a strong statement of intent that defines the PF's individual goals for risk management. The policy should also include objectives that are intended to help the PF achieve that goal, such as a list of MCCs and descriptions of the submerchant industries for which the PF will (or will not) provide service. Special risk management considerations that are appropriate for you based on your established business plan and risk tolerance should be identified. If you provide services to submerchants that present a higher level of perceived risk to the card acceptance ecosystem, such as those described in Section 3: Submerchants Requiring Enhanced Underwriting Due Diligence, then additional, appropriate due diligence considerations should be included in the policy and further described.

### 4.3. The Objectives of Submerchant Risk Management

The PF's policy should include its objectives of submerchant risk management. Such objectives should be to:

- Identify and investigate submerchant activity that is anomalous to your expectations for the submerchant.
- Identify and investigate activity that is anomalous to industry norms for general submerchant.
- Process for defined verticals.
- Ensure submerchant compliance with card scheme requirements.
- Support the identification of suspicious activities, which may be related to money laundering or terrorist financing.
- Identify anomalous activity and file a suspicious activity report (SAR) with the Financial Crimes Enforcement Network (FinCEN) or bank when appropriate.

### 4.4. Activities That Support Submerchant Risk Management Goals

The PF's policies should include activities in support of submerchant risk management, business goals and objectives. Such recommended activities may include the below, which will be described in further detail throughout this section of the guidelines.

Monitoring of submerchant transaction activity to identify exceptions to the underwritten parameters or exceptions to what is considered normal as defined by industry (based on MCC), submerchant business vertical, or individual portfolio averages for the PF. Particular focus should be given, but not limited, to unusual activity in:

- Sales.
- Refunds, especially refunds with no offsetting sale.
- Chargebacks.
- Automated clearing house (ACH) rejects.
- Card present versus card not present ratios.
- Swipe versus keyed ratios.
- Authorization activity, including brute force attacks/testing.
- Average ticket.
- Submerchants should be questioned regarding identified exceptions:
  - You should understand the submerchant's business and marketing practices in their entirety, including not only the transaction or product but also any regulatory and consumer satisfaction implications.

- Further investigation should be completed as deemed necessary.
- Action should be taken based on findings up to and including submerchant closure.

### 4.5. Submerchant Risk Management Policy Effective Standards, Tools and Strategies

Submerchant risk management policies should establish your expectations for the process of monitoring submerchant activity. As recommended for the submerchant underwriting policy, the risk management policy should include proper and well-documented approval authorities and escalated exception processes.

#### 4.5.1. Time Frames

Each PF should establish expected timeframes for review and submerchant notifications of review and adverse actions. Review is required to occur daily (working days) for transactions and at least monthly for the total submerchant activity and trending.

#### 4.5.2. Adverse Actions

Each PF should establish standards regarding adverse actions to take during investigations and if such action should be reported to the acquirer, which may include:

- When funds should be held during an investigation.
- When an account should be temporarily suspended.
- When an account should be terminated, including whether or not a submerchant should be added to MATCH and the timing of such MATCH additions.
- How and when the submerchant should be notified.

#### 4.5.3. Approval Authority Parameters

Designated staff approving authority levels for funds release or parameter changes should include:

- Title and/or position but not an individual's name.
- Funds release request and approval limits.
- A requirement to specify approval notation on the submerchant record.

#### 4.5.4. Escalation Requirements

Circumstances requiring escalated approval should be included. Examples of such circumstances are:

- Submerchant parameter increases in dollar volume/number of transactions processed during a specific time frame at the individual and cumulative transaction level.

- High seasonal volume.
- Alternating high and low months of volume.
- Funds released from submerchant reserves.
- Funds released from suspension.
- MCC codes changes.
- Type changes.
- Processing method changes (for example, keyed to swipe, retail to MOTO, MOTO to e-commerce).
- Marketing methods changes.
- Submerchant bank account changes, including large submerchants with bank account changes.
- More changes than any established policy threshold within a specific time frame.

#### 4.5.5. Documentation Requirements

Each PF should have a designated exception notation format as well as designated review and documentation processes to ensure consistency in reviews and meeting requirements. It is recommended to use a standardized form for consistency of documentation. Examples of the items that could be included in the process and documented are:

- The name and title of the person requesting the exception (differentiate between sales representative, risk analyst, and submerchant).
- The reasons for the exception request.
- The name and title of the person reviewing the request.
- Notation of the exception or change request on the submerchant record with the reason for approval or decline.

#### 4.5.6. Periodic Reporting of Exceptions to Policy

Establishment of periodic reporting of all requested exceptions is recommended to be generated on a monthly frequency. Examples of the items this reporting could contain are listed below:

- Requestor name and title.
- Reasons for decline, if applicable.
- Exceptions approved.
- Reviewing/approving individual, name and title.
- Conditions required for approval.
- Funds released.
- Other actions taken.

#### 4.6. Team Communication

It is recommended that all departments/teams within your organization that are focused on prevention of financial loss and mitigation of fraud and illegal/prohibited activity meet on a regular basis. Such teams may include underwriting, risk, compliance, chargeback and collections, if these processes are separately managed. During these meetings, the teams should share information on identified trends to support ongoing earlier detection and mitigation of potential issues. These teams should also perform joint postmortem exercises on large losses or repeat loss patterns.

In addition to regular team meetings, communication channels should be defined by each PF as appropriate for business processes, which may include when:

- The original underwriter should be included in a risk review.
- Chargeback activity requires additional risk review, if managed separately.
- Situations escalate as defined by your individual risk management policies and procedures.

Forms of communication may include:

- Emailing submerchant account notes.
- Providing copies of team activity and submerchant trend reporting.
- Providing copies of management reporting indicating fraud trends.

#### 4.7. Effective Tools and Strategies for Daily Exception Monitoring

This section will provide suggestions for potential exception parameters that may be set in an exception-based system, including factors based on parameters such as volume, card acceptance method, geography, and MCC, among many others.

The recommended practices in section 4.8 discuss how exceptions should be investigated, once generated.

These recommendations are not meant to be an exhaustive list of potential exceptions as individual portfolio or vertical characteristics often dictate specific triggers that may not be useful elsewhere. PFs may choose to include suggestions from this section, or may determine additional or alternative exception criteria as best fits individual business needs. As with all triggers and exceptions, the PF should continually monitor for relevance and effectiveness. If any trigger or exception is

providing a large amount of false positives, they should be removed or changed either at the portfolio or submerchant level as appropriate.

#### **4.7.1. The Submerchant Record**

The submerchant record should contain approved processing parameters and demographic information that may be used to establish system flags for anomalous activity. Flags that trigger exceptions may be set at many different levels. Some parameters may not be listed individually on the record but may instead be calculated systemically based on a single approved parameter. For example, expected daily, weekly or monthly processing averages can be determined from the approved annual volume or transaction count.

Further calculations may be made based on established acceptable or average portfolio, MCC, vertical or other thresholds for different types of activity, such as refunds or chargebacks as a percent of overall activity. These PF guidelines provide suggestions for defining exception triggers and flags and the resulting actions that may be taken by individual PFs. Nonsubmerchant-specific parameters based on geography, MCC and sales method have been suggested, which may also be useful.

#### **4.7.2. Submerchant Risk Classification Exceptions**

Submerchant risk classifications may be used to generate exceptions based on the existence of circumstances known to present higher risk in processing or may also be used to increase the priority of the submerchant parameter flags, as a higher submerchant risk classification may result in a more restrictive exception tolerance for approved submerchant parameters than the general submerchant population, as discussed in further detail in Section 5: Risk Management For Submerchants Requiring Enhanced Due Diligence.

The following suggested exceptions are highly subjective and specific to each PF's individual portfolio; however, some examples of categories that may be used to create these types of exceptions include the following.

##### **4.7.2.1. Micro and/or Mobile Submerchants Monitoring Recommendations**

The underwriting on this submerchant category is typically frictionless and completed in stages. When staged underwriting is employed, the first transaction should be reviewed to ensure the submerchant is processing as approved. As always, the first 90 days of processing should also be closely monitored.

##### **4.7.2.2. Restricted Submerchants Monitoring Recommendations**

Restricted submerchants should have thresholds set more strictly to monitor any deviation from the approved activity for the account, regardless of general system thresholds.

##### **4.7.2.3. Submerchant Watch List/Monitored Submerchants Monitoring Recommendations**

Submerchants may be designated for close monitoring based on processing volumes, business type, marketing methods, cardholder complaints or prior processing issues such as past refund or chargeback spikes by the underwriter as discussed in Section 2.7, or from prior risk investigations.

While not technically defined as a restricted submerchant, these submerchants may be granted conditional processing requiring usage of various fraud control tools such as AVS, CVC2/CVV2, IP tracking, 3D Secure, (Visa: VCAS (Visa Consumer Authentication Service); MC: Secure Code), or affiliate monitoring; or require strict adherence to approved parameters. Similar to restricted submerchants, monitored submerchants should have closely set thresholds with less room for variance.

##### **4.7.2.4. Other Risk Classification Criteria Recommendations**

Additional types of higher risk submerchant classification that you may consider, as appropriate for your submerchant portfolio, may include:

- Product type
- Sales method
- Delivery time frames
- Marketing method
- Submerchant location (high-risk areas such as those suggested in Section 3.6)
- Newly identified fraud trends that trigger a thorough systematic portfolio review to find existing submerchants who may qualify

#### **4.7.3. Daily Exception Reports Effective Tools and Strategies**

Exception reports may be based on overall scoring or individual parameters, as determined appropriate by each PF. Regardless of the basis for exception, the items generated should be reviewed and actioned daily. While the list below is not exhaustive, it contains suggestions of practices that may be used when monitoring transactions on a daily basis. PFs may also take other reasonable steps to properly monitor daily exception reports so as to minimize risks. Exception review

priority should be determined by each PF and documented in risk policies and procedures.

#### 4.7.3.1. New Submerchant Exceptions Recommendations

New submerchants are generally considered to be those which have begun processing within the last 90 days; however, some PFs may choose to extend this to 180 days or more, as appropriate for the individual submerchant portfolio and submerchant risk classification. Additionally, you may choose to treat accounts that have been dormant for a pre-determined period of time, such as 90 days, as new submerchants for purposes of monitoring new processing activity after dormancy.

New submerchant activity should also be compared to the average processing activity for the assigned MCC, or submerchant vertical, if applicable.

#### 4.7.3.2. New Submerchant Volume Based Exceptions Recommendations

Further exceptions that should be reviewed for new merchants are:

- Daily cumulative deposits should generate an exception at 150% of the expected average daily amount, based on approved monthly volume.
- Individual batch deposits (if a submerchant batches more than one time per day) should generate an exception at 150% of the expected average daily amount, based on approved monthly volume.
- It is recommended to determine tiers for processing levels for closer monitoring of volume with respect to the individual submerchant risk to the entire portfolio, for example:
  - Larger submerchant activity, as defined by each PF's underwriting risk levels according to Section 2.4, should generate a daily exception when cumulative monthly sales volume reaches 90% of approved monthly volume.
  - If the percentage (%) is reached in the first three-quarters of the month, the submerchants should be more diligently reviewed.
  - It is recommended that this threshold be set lower for higher risk submerchants.
  - Smaller submerchants representing less risk exposure should generate exceptions on a tiered basis when cumulative monthly sales volume reaches 100% to 300% of their approved volume as makes sense based on each PF's individual portfolio, for example:
    - 100% for large/graduating submerchants
    - 150% for medium submerchants
    - 300% for micro/mobile and small submerchants

#### 4.7.3.3. Volume Increases/Processing Spikes Exception Examples

Daily deposit amount exceeds expected amount based on approved monthly volume.

- For recurring billing submerchants, you may choose to inactivate this exception.
- Month-to-date volume exceeds prior month's volume.
- Month-to-date volume exceeds monthly average over the past 90 days.
- Rolling 30-day volume.
- Calculated as a measurement of the last 30 days' processing volume compared to expected average monthly volume.
- Reflected as a percentage (%) of rolling 30-day volume/ average monthly volume.

#### 4.7.3.4. Volume Decreases/Processing Dips Exception Examples

For submerchants in the defined medium or large category of processing volumes, scrutiny should be given to deviations of normal and typical volumes:

- Rolling 30-day or month-end volume has decreased by 20% or more compared to the previous rolling 30-day period, month-end processing volume, or average monthly volume over the previous 90 days.
- Calculated as a measurement of the last 30 days' processing volume, reflected as a percentage (%) of the comparison parameter.
- The first 15 days' processing for the month has increased or decreased from the prior month by 20% or more.
- Volume has increased or decreased by more than 25% from week to week.

#### 4.7.3.5. Batch Activity Exception Examples

- Batch net amounts
- Zero net dollar batches
- Negative net dollar batches
- Changes to the frequency of submerchant deposits

#### 4.7.3.6. Individual Ticket/Sale Exception Examples

Based on card scheme recommendations, the activity described here is suggested to generate exceptions when the activity reaches 150% above the expected parameter as determined by underwriting or at a different percentage that is appropriate for the risk tolerance of the PF, as well as the submerchant processing level and type.

- Tickets over maximum approved amount.
- Individual ticket equal to or greater than an amount commensurate with each PF's individual risk tolerance.
- The exception trigger should be set as appropriate for the proportion of risk that the ticket size represents compared to the portfolio, total transactions and processing volume of the PF; for example:
  - Some PFs with less risk tolerance may choose to view all tickets processed that are greater than a predetermined dollar amount, regardless of whether that ticket is over the individual submerchant's expected maximum.
  - Average ticket dollar amount is not as expected or is outside a tolerance established by the PF. It is common practice and recommended to include this parameter in the submerchant record. This parameter may be set to trigger based on monthly average, daily average or batch average, as determined by the individual PF.
  - The average count of tickets processed is not as expected or outside a tolerance established by the individual PF. The average count of tickets may be calculated based on the approved annual volume and average ticket. This may also be set at monthly average, daily average or batch average, as determined by the individual PF.
  - Multiple small-dollar transactions (recommended to be less than \$3), which are not within the submerchant's approved parameters.
  - Excessive percentage of card present versus card not present transactions outside of the submerchant's approved parameters.
  - Excessive percentage of keyed transactions outside of the submerchant's approved parameters.
  - Multiple transactions from the same bank identification number (BIN), which is the first four to six numbers of the cardholder's number. This may be set at a percentage of the batch for those with a higher risk tolerance or at a hard number, such as four, for those with a lower risk tolerance.
  - Multiple transactions from the same or similar card numbers.
  - Same-sale dollar amount transactions repeated in the same batch that is out of pattern for the submerchant. This may be set at a percentage of the batch for those with a higher risk tolerance or at a hard number, such as four, for those with a lower risk tolerance.

#### 4.7.3.7. Foreign Activity Exception Examples

Transactions on non-U.S. issued cards that are out of pattern for the submerchant. It is recommended to set an expected

percent of foreign transactions or number of foreign cards in a batch on the submerchant record.

#### 4.7.3.8. Authorization Activity Exception Examples

- Forced authorizations/ticket-only transactions.
- Authorization reversals.
- Authorization activity with no captured sales.
- Multiple transactions with the same authorization number.
- Multiple authorizations for the same card and/or cardholder.
- Total daily authorization count compared to account parameters.
- Repeated declines on the same card number.
- Repeated declines on the same BIN. Daily authorization declines exceeding parameters set for the industry.
- It is common for recurring sales submerchants to have decline ratios up to 30%, and it is recommended to set that as the tolerance level unless additional risk factors exist.
- It is not common for retail sales submerchants to have greater than 5% decline ratios.
- Attention should be given to high ratios of certain decline reasons determined by each PF to be of concern within overall transaction declines.
- 10% "pick up card" as a reason for decline should be investigated, as the submerchant may be a victim of fraudulent card usage.

#### 4.7.3.9. Abnormal Transaction Time Frames Exception Examples

- Unusual transaction times based on submerchant's hours of business.
- Unusual transactions based on seasonality of the submerchant.

#### 4.7.3.10. Submerchant Changes Exception Examples

Each PF should define submerchant changes that would require review by risk management staff and whether the review should be done prior to change completion or following completion for cursory review.

The following types of submerchant account changes are suggested to be carefully reviewed as they may indicate a beneficial owner or fraudulent account application information was provided. Particular attention should be paid to activity happening within 30 to 60 days of account opening or periods of dormancy of greater than 90 days.

- Submerchant DBA changes

- Legal or tax ID changes
- Descriptor changes
- Any phone number changes
- Address changes
- Website changes
- DDA changes

#### 4.7.3.11. Refund/Credit Transaction Exception Examples

Refund exception tolerances may vary based on the different types of submerchants using averages based on MCC, sub-merchant verticals and portfolio demographics and should be determined by the individual PF. Numbers provided in the examples below are based on input from the working group across the acquiring industry.

- PFs should also implement logic to require all refunds be linked to an original sale transaction record. Unlinked credits should also be monitored to ensure the transaction type is not being used in a noncompliant manner.
- Refund percentages should be calculated on both the dollar volume and count of refund compared to transaction processing as previously defined.
- It is recommended to tier exception generation based on refund volume, submerchant processing volume, and/or submerchant risk classification, as applicable for the PF, in order to keep monitoring of this activity efficient.
- Examples of some possible tiered exception criteria are listed below. The ratios, dollars and numbers of transactions should reflect each PF's risk tolerance.

#### Card Present Submerchants

- 4% or greater ratios for both dollar volume and item count.
- Refund ratio exceeding 2% with daily total greater than \$5,000 and daily count greater than 5.
- Refund ratio exceeding 3% with daily total greater than \$2,500 and daily count greater than 5.

#### Card Not Present Submerchants

- 8% or greater ratios for both dollar volume and item count.
- Refund ratio exceeding 3% with daily total greater than \$5,000 and daily count greater than 5.
- Refund ratio exceeding 5% with daily total greater than \$2,500 and daily count greater than 5.
- Refunds dollar amounts that are larger than the PF's individual risk tolerance.
- Exceptions may be generated for a single item amount, or for the total amount in a batch/daily total.

- A more risk-tolerant PF may set this at \$5,000.
- A less risk-tolerant PF may set this at \$500.
- If possible, the following should not be allowed to enter interchange:
  - Refunds with no offsetting sale.
  - Refunds issued subsequent to a chargeback on a single account.
  - Increasing refund activity after elevated chargeback issues.

#### 4.7.3.12. ACH Reject Exception Examples

Review all ACH (automated clearing house) rejects along with their reason codes when available (debit or credit). Note: This references ACH debits related to credit card processing (PFs billing monthly processing and other fees), not third-party ACH processing.

- Daily
- Monthly ratios

#### 4.7.3.13. Retrieval Request Exception Examples

- Daily, weekly or month-to-date retrievals that exceed the PF's predetermined percentage of the submerchants processing volume or transaction count.
- Retrieval requests for card not present submerchants.
- Retrieval requests with reason codes determined to be of concern.
- Requests for a large-dollar transaction or total dollar amount of transaction(s) for a single day or batch that is out of the typical range for the submerchant.

#### 4.7.3.14. Chargeback Activity Exceptions Recommendations

- Monthly ratios
- Chargeback dollar amounts that are larger than the PF's risk tolerance.
- Single chargeback.
- Total daily amount of chargebacks.
- Month-to-date cumulative chargeback totals.
- Daily exception review is typically based on dollar volume. Examples of some possible tiered exception criteria based on monthly percentages can be found in Section 4.8.
- Examine the chargeback reason codes and supporting documentation to determine whether the concern is:
  - Financial risk – the submerchant being able to cover activity.

- Consumer fraud against the submerchant (e.g., the submerchant is a target of fraudulent card usage).
- Submerchant fraud against the consumer. The submerchant is billing the card without shipping or delivering the product, or the submerchant is making unauthorized charges to the consumer's account.
- Product quality.
- Operational issues such as shipping or customer service.
- Marketing issues such as potential misrepresentation to the consumer.

#### 4.7.3.15. Fraud Prevention Tool Response Exceptions

- Address verification
- Card acceptor ID (CAID), Card Verification Value, CVV2, Card Verification Code, CVC2
- MC secure code/Visa VCAS
- Device authentication
- IP tracking
- Restrictions on ship-to countries

### 4.8. Effective Tools and Strategies for Monthly or Periodic Exceptions

It is recommended that monthly or other periodic exception reporting for critical risk activity, as determined by each PF, be generated for review by more senior or experienced risk staff. This may serve to identify activity that may not have been given high priority during daily exception review but that taken as a whole over the longer time frame becomes a concern and may serve to summarize the monthly activity for the team and identify areas where training may be of benefit.

#### 4.8.1. Top Processing Volume, Chargeback Volume, or Refund Volume Report

- Include cumulative totals for related or chained submerchant accounts (i.e., one legal entity with 10 accounts that when combined are within the defined review group).
- When reviewing chain submerchants, also review each location to ensure single location issues are not being hidden by other locations.
- Documented review should take place using a standardized review format containing:
  - Refunds (review the dollar, number, and percentages): month, prior month, year-to-date (YTD).
  - Chargebacks (review the dollar, number and percentages): month, prior month, YTD. Review should include

all outlier submerchants, especially those who are in card scheme chargeback monitoring programs (pre or post fines).

- In-depth product/service review.
- Website review.
- Social media review.
- Consumer satisfaction review (Better Business Bureau, online complaint boards).
- Copy of periodic review, if available.

#### 4.8.2. Reports by Submerchant Vertical (MCC, Product Type, Agent/Agent Group)

Each PF should define verticals specific to its portfolio.

- PFs should establish thresholds for review and additional investigation appropriate for the industry vertical.
- PFs should review the verticals on a six-month rolling basis and investigate significant increases and decreases.

#### 4.8.3. Restricted Business Type Review Monthly Report

It is recommended that submerchant exceptions for restricted business type submerchants be summarized at the end of the month for summary review by more senior-level risk management staff. Examples of restricted submerchants could include:

- Furniture, flooring, travel (i.e., all future delivery).
- The processing volume, chargeback volume or refund volume that triggers the restricted submerchants for review should be lower than that which triggered the not-restricted submerchants.

#### 4.8.4. Monthly Excessive Volume Exceptions

Submerchants that have larger processing volumes or exposure should be reviewed on a periodic basis. At a minimum, the review should be annual, but if the statistics demonstrate enhanced diligence is required, the review could occur as often as monthly. Such reviews may be scheduled semi-annually, quarterly or monthly. If the submerchant is also being reviewed as defined in Section 4.8 for a periodic review or Section 6.2 for graduation, the two reviews could be combined.

#### 4.8.5. Submerchants With Decreasing Volume

The purpose of this report is to monitor submerchants with significantly decreasing (or stopped) volume that may not otherwise be detected through monitoring of daily activity.

- Monthly report of the sales activity that has decreased by a predetermined percentage from the prior month.

- Can be narrowed down to submerchants processing over some larger amount per month as determined according to the PF's risk policies.
- Submerchants who processed some predetermined volume in the prior month but had no processing in the report month.

#### 4.9. Submerchant Graduation Review

Each submerchant must be monitored daily to detect when processing has reached the card scheme thresholds. If the conditions are met, refer to section 6.2 to properly graduate the submerchant from the PF program. Card scheme volume thresholds for submerchants are currently established as:

- Visa processing reaches \$100,000 in one calendar year or
- MasterCard processing reaches \$1,000,000 in one calendar year.

Based upon these limits, the PF should review submerchants who have reached PF defined daily, weekly, monthly and YTD processing thresholds for Visa or MasterCard. The PF should set the threshold below the card scheme limit listed above to ensure graduation as defined in Section 6.2 can be properly executed.

#### 4.10. Submerchant Changes

As recommended in Section 2.6, each PF should define types of submerchant account changes that should be reviewed in a summary monthly report by more senior-level staff, particularly those made for submerchants that represent greater exposure to the PF. The review is recommended to be cursory and act as a second set of eyes on changes that occurred throughout the month. Particular attention should be paid to activity happening within 30 to 60 days of account opening or periods of dormancy of greater than 90 days, for activity such as:

- Submerchant DBA changes
- Descriptor changes
- Any phone number changes
- Address changes
- Website changes
- DDA changes

#### 4.11. Monthly Refund Exception Effective Tools and Strategies

Based on the increased scrutiny of submerchants through UDAAP, it has become more important to monitor the refund

ratios of all submerchants. Regular monitoring of the ratios based on business and processing-type averages along with consumer complaint boards and online blogs will give the PF insight into the submerchant. The ratios below are based on industry research and may be adjusted by each PF to better reflect individual portfolios, and submerchant refund monitoring policies should be well documented to inform the analysts of the guidelines that should be followed. Submerchants' records should also be noted when it is acceptable that they are outside of the chosen parameters, including the degree of exceptions approved and the reasons why. Such notes should include consumer satisfaction review when appropriate, as a high-refund ratio can be a barometer for consumer dissatisfaction. The parameters below should be reviewed for both the number of transactions as well the dollar volume of transactions in the given time period.

##### 4.11.1. Refund Monthly Exception Thresholds

Trending reports should be reviewed at least monthly and should be reviewed more often for portfolios with submerchants that could generate more consumer complaints. In addition to the quantity/dollar ratios, attention should also be paid to trends in time lapse between date of the credit/refund and the original sale date.

###### 4.11.1.1. Card Present Submerchants

- 4% or greater ratios for both dollar volume and item count
- Refund ratio exceeding 3% ratios and
- Monthly total greater than \$25,000
- 75 or more refunds
- Refund ratio exceeding 2% ratios and
- Monthly total greater than \$50,000
- 150 or more refunds

###### 4.11.1.2. Card Not Present Submerchants With 8% or Greater Refund Ratios

- 8% or greater ratios for both dollar volume and item count
- Refund ratio exceeding 5% ratios and
- Monthly total greater than \$25,000
- 75 or more refunds
- Refund ratio exceeding 3% and
- Monthly total greater than \$50,000
- 150 or more refunds

## 4.12. Monthly Chargeback Exception Effective Tools and Strategies

Based on the increased scrutiny of submerchants as a result of UDAAP laws, it has become more important than ever to monitor the chargeback ratios of all submerchants before they reach card scheme monitoring levels. Monitoring the chargeback ratios based on MCC and processing type averages along with consumer complaints and blogs will give the PF insight into the submerchant. PFs should review in aggregate as a dual check with elevated refund ratios to ensure that the submerchant is not issuing refunds to avoid detection in PF card scheme monitoring programs.

The ratios below are based on input from the working group and may be adjusted by each PF to better reflect individual portfolios and submerchants. Each PF should document its established thresholds to provide analysts with guidelines that should be followed. Submerchant records should also be noted when activity exceeding established thresholds will continue to be allowed, including the degree of exception approved and the reasons why. The parameters below should be reviewed for both the number of transactions as well the dollar volume of transactions in the given time period. PF best practices should stress and address timely review, early detection and remediation, as all are critical to mitigating risk exposure, brand damage and assessments.

### 4.12.1. Chargeback Reporting Threshold Examples

Examples of some possible tiered exception criteria are:

- Chargeback ratio exceeding 2.50% and 25 or more chargebacks
- Chargeback ratio exceeding 0.75% and 75 or more chargebacks

### 4.12.2. Chargeback Management Reporting

A monthly report of top chargeback submerchants is recommended to indicate individual or groups of related submerchants that represent a large percentage of the PF's portfolio's total chargeback volume in order to identify high chargeback volume accounts that may be within acceptable parameters but still should be reviewed based on the portion of the portfolio represented.

- Should be calculated for both dollar amount and number of chargebacks.
- Trending reports should be reviewed at least monthly and more often for those submerchants with more consumer complaints. An example has been provided as Exhibit E.
- All chargeback reports should include both individual submerchant accounts that meet the parameters and chained

accounts grouped by legal entity or mutual ownership that also meet the parameters.

As previously stated, the recommendation is to remediate issues prior to the submerchant reaching a chargeback activity level that qualifies the submerchant for remediation programs defined by the card schemes. As such, each PF should individually determine the appropriate thresholds by which to identify submerchants within the PF's portfolio that is lower than the defined thresholds for the card schemes.

### 4.12.3. Card Scheme Risk Monitoring Program Submerchants

Submerchants that are currently in card scheme risk-monitoring programs should be reviewed for root cause detection and closely monitored by senior risk management staff with monthly status reporting and month-over-month status and statistical changes reviewed. Please refer to each specific card scheme's published rules for its respective program parameters.

- Fraud monitoring programs
- Chargeback monitoring programs

In instances where the submerchant does not cure the root cause of the program violation, a PF may be required to terminate the submerchant relationship. PFs should review whether or not the terminated submerchant should be added to MATCH.

### 4.12.4. Chargeback Monitoring and Investigation Procedure Effective Tools and Strategies

Based on the established importance within these PF guidelines for mitigation of chargeback issues, the intent of this section is to provide guidance for ways to review and action chargeback exceptions. These recommendations are appropriate for the management of both the daily chargeback exceptions in Section 4.7 and for the submerchants included in the monthly or periodic management reporting in Section 4.16.

Following these recommended practices should help ensure that unmitigated chargeback issues do not create undue harm to consumers or the card acceptance ecosystem.

### 4.12.5. Chargeback Monitoring Team

- It is recommended to establish dedicated investigators to monitor chargebacks separately from transaction monitoring. If such monitoring is of a higher risk portfolio, ensure the investigators are tenured. A PF that generates less than 5,000 chargebacks per month across its entire portfolio may not need to separate the function from the risk monitoring and loss prevention department.

- A well-defined communication structure between risk analysts and chargeback analysts should be created as defined in Section 4.6.
- Chargeback exceptions as defined in 4.7.3.14 should be monitored daily by the established team or individual(s).
- Monthly or periodic reporting for chargebacks outlined in section 4.8 should be monitored by this team.

#### 4.12.6. Chargeback Activity Monthly Projections

- You should project what the month-end chargeback count and amount will be based on activity received month to date  $[(\text{dollar or items received} / \text{days elapsed}) * (\text{total days in month})]$ .
- You should compare the projected chargeback count and amount against average monthly transaction count and amount to determine potential chargeback ratios.
- You should compare the month-to-date and projected month-end chargeback count, amount and ratios to the prior month.
- You should compare a trending of the last six months as defined in Exhibit E.

#### 4.12.7. Chargeback Detail Review Recommendations

- You should understand truly fraudulent card usage versus submerchant error versus submerchant engaging in UDAAP law violations.
- You should review and monitor chargeback reason codes. Certain reason codes may be uncharacteristic for a business model or MCC, while others may be an early detection of bust-out, financial distress or change of product types.
- Fraud.
- Operational issues.
- Customer dissatisfaction with product. Where available, it is wise to review cardholder comments provided with dispute documentation.
- Ensure information is consistent and characteristic of the submerchant's business model.
- You should review the chargeback supporting documentation.
- Look for potential consumer deception claims.
- Ensure the product at issue was approved for the account.

### 4.13. Effective Tools and Strategies for Investigating Exceptions

The PF's policy should have a section that clarifies the steps to be taken when investigating a specific transaction and/or the submerchant.

#### 4.13.1. The Purpose of Investigation

PFs should determine whether factors that systemically have flagged an account for review indicate a likely risk of financial loss for you or the processing of illegal or prohibited transactions by the submerchant. Some examples include but are not limited to, the submerchant's use of potentially deceptive marketing practices or transaction laundering.

Activities that support this purpose include:

- Verification that the transaction submitted is as approved (ensure they have not changed product, sales method or resulting MCC).
- Verification that transactions are submitted in accordance with card scheme rules.
- Determination and mitigation of fraudulent card usage.
- Determination and elimination of consumer deceptive practices.
- Verification that the submerchant's current financial condition remains as expected or is further sufficient to cover excepted activity.

#### 4.13.2. Documenting the Investigation

It is a recommended practice that decisions made regarding the activity be documented as to the thought process when action is taken.

Although it is not necessary to document when no action is taken, an effective tool is to document when there are repeated exceptions for the same type of item and no action is taken. This may become very important when reviewing anomalous chargebacks or refunds. If a submerchant has continually high or anomalous statistics and no action is taken, the submerchant record should be clearly noted as to why no action is necessary.

#### 4.13.3. Investigation Basics

All submerchants meeting exception criteria based on identified thresholds or who are designated for monitoring should be investigated to determine whether the activity presents risk of financial loss to the organization or whether the possibility of illegal, prohibited or deceptive practices exists. Investigations may vary in scope depending on the type of exception(s) flagged and additional information discovered.

Investigation activities may include:

- Increase of scope beyond identified exception review to include a holistic review of the submerchant.
- Contact with the submerchant.
- Request transaction supporting documentation whether the investigation is for a sale, refund or chargeback.
- Interview the submerchant regarding the exception(s) identified.
- Do not suggest scenarios when discussing the exception with the submerchant.
- Ask open-ended questions.
- Verification of card/cardholder details with issuing bank(s).
- Reviewing the submerchant sales methods.
- How products/services are marketed (refer to Section 5.8 for specifically identified high-risk marketing methods and how to review).
- Secret shopping (refer to Section 5.4).
- Reviewing the submerchant's usage of common fraud prevention response tools, which may include:
  - Address verification
  - Card acceptor ID, Card Verification Value, CVV2, Card Verification Code, CVC2
  - MC SecureCode/ Visa VCAS
  - Device authentication
  - IP tracking
  - Restrictions on ship-to countries.

The following is a noncomprehensive list of example actions that could be taken following investigation:

- Require the submerchant to issue a refund.
- Place the submerchant on increased monitoring for future occurrences.
- Hold funds from the excepted activity.
- Suspend the submerchant's ability to process any transactions.
- Suspend the submerchant's ability to process refunds.
- Require the submerchant to change its website.
- Require the submerchant to discontinue the sale of a specific product.
- Require the submerchant to open a separate submerchant account.
- Implement daily discount of submerchant account fees.
- Implement ongoing deposit delays.

- Other actions that may be required to mitigate the exception risk.

#### 4.14. Submerchant Remediation

Each PF should gauge whether the issues requiring remediation can be fixed. For example, if the issue is an inherent product or service issue, it may not be able to be corrected, but if the issue is customer service related, then upgraded systems, training or additions to the submerchant's staff may help remediate the issue. An example of time frames for remediation would be to review the progress in 30-day intervals with a goal to see improvement within 60 days (depending on the issue). Some issues may take up to 90 days to be corrected. It should be expected that the majority of issues should be corrected within six months. PFs should consider termination of a submerchant if an issue cannot be corrected within six months.

#### 4.15. Submerchant Reserves

While reserves may be used as protection in an escalating risk situation, they should not be used as the sole determinate in whether to keep a submerchant open or to close the submerchant. In most cases, submerchant volumes, MCC or product delivery should not pose risks such that reserves should be accrued on a rolling or sustained basis. Reserves should not be used as a way to manage submerchants engaging in acts or practices that a PF feels are, or that legal counsel considers, potentially unfair, deceptive or abusive to consumers. In lieu of allowing any such submerchant to process with a reserve, the submerchants should be denied the ability to continue to process.

As the practice of reserves is limited in the risk management of submerchants, PFs should consult the ETA Guidelines on Merchant and ISO Underwriting and Risk Monitoring for expanded materials and guidance.

#### 4.16. Monthly Management Reporting Effective Tools and Strategies

The establishment of monthly management reporting is important to ensure that there is appropriate senior-level oversight of the day-to-day activities within risk management. Monthly reporting should provide a high-level summary regarding activity deemed by each PF to warrant management or senior-level attention. PFs with large portfolios may wish to create separate levels of reporting requirements for respective management levels.

At a minimum, senior management should review reporting that is required to be presented up to the next-level organization. Section 6 provides more information about the risk management reporting that is recommended for PFs who sponsor submerchants.

The report types provided in this section are meant to represent typical management summary reporting available in the industry for reference by PFs. Each PF should determine what types of reporting are appropriate for individual use.

## 5. Risk Management for Submerchants Requiring Enhanced Due Diligence

Submerchants requiring enhanced due diligence, which are also known as higher risk (HR) submerchants, are manual and labor intensive, as they often require additional monitoring and staffing responsibilities. Some HR submerchant types have additional mandatory registration requirements with the card schemes. (Please note that registration is outside the scope of this document. To determine all circumstances when a PF should be registered with the card schemes please refer to the card scheme rules.) Sponsoring HR submerchants typically requires a more robust and knowledgeable staff.

Higher risk submerchants also carry a higher probability of reputational risk, and in some cases, there is a higher risk to the card acceptance ecosystem for all players on the acquiring side as well as the cardholder. Due to this increased risk, this next section describes extra diligence that should be taken at minimum, in addition to the minimum requirements prescribed by card schemes and applicable laws and regulations.

### 5.1. Enhanced Due Diligence Process

In addition to the effective strategies outlined in this Section 5, the recommended practices discussed in Section 3.0 for Underwriting of Submerchants requiring enhanced due diligence apply here as well. When reviewing higher risk submerchants in these categories, it is an effective risk mitigation practice to investigate fully, notate the submerchant file completely, and take action concretely. If a submerchant does not take the requested corrective action in the requested amount of time, the submerchant account should be closed. It is not a recommended practice to increase reserves or charge fees to offset the lack of corrective action.

### 5.2. Performance Improvement Expectations

It is appropriate to expect that the submerchant take corrective action within 30 days after you request action, with the resulting improvement in processing statistics to be seen within three months and no longer than six months after the request. It is recommended to close a submerchant account if sufficient improvement is not seen within the time frames noted in each PF's policies and procedures.

When reviewing the effects of the corrective actions taken by a submerchant, you should see, at a minimum, an improvement in:

- Chargebacks.
- Refunds. As a best practice, PFs should implement logic to require all refunds be linked to an original sale transaction.
- Customer complaints.
- Once improved, the submerchants should remain on your watch list for at least six months.

### 5.3. Reputation Monitoring

A plethora of information is available online for reviewing consumer perception regarding a submerchant. This is an easy way to investigate submerchants, particularly those representing potential higher risk due to marketing or sales methods, product type or operational issues.

- Examples of types of online resources:
  - Consumer complaint boards
  - Better Business Bureau (BBB)
- Online searches may be performed using keywords related to the submerchant account, including:
  - Legal name/DBA
  - Product or service name
  - Submerchant account descriptor
  - Website URL
  - Phone numbers
  - Email addresses

### 5.4. Secret Shopping

Secret shopping is a tool that may be used at the PF's discretion as a verification method to ensure submerchant compliance with card scheme requirements, submerchant account conditions, and that general consumer satisfaction practices are in place.

With secret shopping, random purchases are made to assess the products or services received and ensure they are as described on the submerchant application. The product should then be returned (or the service cancelled) and the return and refund process evaluated for ease of use and quality of customer service. All findings should be analyzed and clearly documented in the submerchant file.

This process helps ensure the product is as described and that no deceptive advertising exists. This process also ensures

that the amount charged matches what was indicated during underwriting and that no additional fees were charged. The return process ensures that the consumer is being treated fairly and receiving the refunds promised.

The secret shopper experience should then be compared to the social media research findings and other website review findings. The combination of these review types could assist in determining the overall risk presented to the cardholder and the card acceptance ecosystem by the submerchant.

A reserve should not be used in lieu of closing a submerchant with negative secret shopping results.

### 5.5. Cardholder/Customer Interviews

The cardholder contact information received from the submerchant during transaction validation should be compared to information found online to ensure consistency. When interviewing the cardholder:

- Ask open-ended questions. Do not suggest purchase or transaction scenarios, and do not suggest issues that may prompt chargebacks.
- Ask for the URL from where the customer purchased the product, and ensure it matches the URL you have on file.
- If the customer returned the product, ask open-ended questions about the return process and the customer's satisfaction.

### 5.6. Chargeback Monitoring and Reporting to Card Schemes

While it is important to understand the card scheme chargeback monitoring programs, this document does not speak to those programs, as it is the intent that if these PF guidelines or some other reasonable step or strategy identified by PFs are followed, any systemic submerchant chargeback issues will have been resolved, or the submerchant will have been closed prior to entering into or persisting in a program.

The review of each submerchant according to internally defined chargeback thresholds could identify accounts with the potential for increased financial risk as well as for identification by the card schemes for violations and subsequent fines.

To understand the details of each card schemes rules, please refer to their specific regulation.

## 5.7. Enhanced Review of the Sales Processing Method

The recommended practices discussed in Section 3.2 for Internet, MOTO, mobile apps and mCommerce submerchants apply here as well. When reviewing higher risk submerchants in these categories it is a recommended practice to investigate fully, notate the submerchant file completely, and take action concretely.

### 5.7.1. Internet Submerchants

#### 5.7.1.1. Website Content Monitoring

- All website pages should be reviewed every 30 days to ensure submerchants are not processing prohibited or illegal transactions. It is a best practice to use a merchant monitoring service provider for website ongoing review.
- Annually review website product, service offerings and disclosures to ensure that there have been no material changes from underwriting approved content as described in Section 3.2. Submerchants with high volume or those on restricted or monitored lists should be reviewed more frequently according to risk tolerances established by your individual policy.
- See Exhibit B for detailed recommendations on reviewing websites.

#### 5.7.1.2. Monitoring Internet Submerchants With Negative Option Marketing

- Website should have a clear and conspicuous disclosure of the terms before the customer agrees to order.
- The action that must be taken by the consumer to avoid further charges should be clearly and conspicuously displayed.
- The action required to be taken by the consumer to cancel should be clearly and conspicuously displayed.
- PFs should consider whether the length of any trial period is reasonable for the product (e.g., at least 14 days for tangible products and 10 days for intangible or digital products).
- The amount and timing of recurring charges should be clearly and conspicuously displayed.
- Disclosures should be in close proximity to the “buy” button.
- The specific card that will be charged should be clearly and conspicuously displayed.
- A PF may monitor for multiple sales on the same card to ensure there are no sales being charged that the cardholder is not aware of.

- Shipping timelines should be clear. (Note: It is typically required by the card schemes that shipping occur the same day the card is charged.)
- You should understand all URLs being used by the submerchant with each submerchant account.
- Refunds should be timely and consistent.

If the submerchant is properly passing the indicator with the transaction that tells you whether it is an initial transaction or a recurring charge, you may track chargeback and refund ratios accordingly.

### 5.7.2. Telemarketing Including Mail Order/ Telephone Order (MOTO)

#### 5.7.2.1. General Transaction Monitoring

- It is important to monitor for multiple sales on the same card to ensure there are not upsells or cross sells that were not approved.
- The ticket amounts must match that expected based on the script review.
- Returns should be timely and consistent.

#### 5.7.2.2. Marketing Monitoring

- Periodic script review
- Secret shopping

#### 5.7.2.3. Telephone Submerchants Negative Option Marketing (Card Scheme Specific Stipulations Exist)

- Scripts should include a clear disclosure of the terms before the customer provides payment information and agrees to order.
- The action that must be taken by the customer to avoid further charges should be clearly explained.
- The action that must be taken by the customer to cancel should be clearly explained.
- The amount and timing of recurring charges should be clearly explained.
- The specific card to be charged and amount that will be charged should be clearly explained.
- The PF should monitor for multiple sales on the same card to ensure there are no sales being charged that the cardholder is not aware of.
- Shipping timelines should be clearly explained.
- Refunds should be timely and consistent.

- If the submerchant is properly passing the indicator with the transaction that tells you whether it is an initial transaction or a recurring charge, you may track chargeback and refund ratios accordingly.

### 5.7.3. Mobile Commerce

- Regardless of the screen size or character limitations, the website should be reviewed just as a nonmobile website, as all requirements are the same.
- The fact that tablet sites have a higher average ticket than smartphone sites should be factored in to the transaction review.

### 5.7.4. Mobile Apps

- The app should be reviewed just as a nonmobile website, as all requirements are the same.
- Ensure the app sells the same product as that which was approved for the submerchant.
- Ensure the app is compliant with all requirements.

## 5.8. Increased and Expanded Affiliate/Affiliate Network Marketing Review

Affiliate marketing is a commonly used type of performance-based marketing for Internet submerchants. In this model, merchants pay “affiliates” (also referred to as “publishers”) for website traffic or sales generated by the affiliate’s own marketing efforts. Some merchants contract directly with individual affiliates, while others contract with “affiliate networks” that manage groups of affiliates working within the network. In the latter model, affiliate networks are responsible for compensating the individual affiliates.

These PF guidelines contemplate that affiliates processing volumes typically qualify these MCCs as direct merchants. Please refer to the Guidelines for Merchant and ISO Underwriting and Risk Monitoring published January 2016 for the detailed overview of the use of affiliates.

## 6. Requirements for Settlement

In the PF processing environment, the acquiring bank funds the PF for settled submerchant funds. The PF then provides downstream funding to the submerchant. As the financial steward for the submerchant, PFs should create appropriate daily and monthly reconciliation practices and role-based desktop procedures that identify gross receipts and other values by submerchant.

PFs are also responsible for recovering submerchant adjustments including chargebacks and refunds against submerchant-settled funds. The PF is prohibited from using the submerchant funds for its own operational purposes. However, should the PF desire, it may net its fees prior to settlement. If PFs delay settlement when specific transactions or batches are triggered for further investigation, such information should be communicated to the submerchant. Additionally, the PF should control and monitor reserves and holdbacks in accordance with the acquiring bank policy. Please note that funds designated are reserves must be held and controlled by the acquirer.

Because the PF is funding the submerchant directly, the PF must also provide statements and proper disclosures to the submerchant. To ensure compliance with the varied state disclosure regulations, it is recommended that PFs seek legal counsel in regard to statement requirements and notification periods.

### 6.1. Guidance on Financial Operations

PFs should maintain role-based procedures and reconciliation practices to ensure submerchant funds settlement, fee calculations, assessments and any adjustments are properly transitioned through the banking systems. Proper daily and monthly practices are critical to ensuring that funds are appropriately settled to the submerchant’s designated bank account.

Additionally, as a best practice, PFs should establish a hierarchy of account structure as directed/recommended by their acquirer. Types of PF accounts necessary to affect submerchant settlement may include:

- Settlement and operating accounts
- Divert accounts
- Restricted cash accounts
- Suspense accounts
- Reserve accounts

PF procedures and practices for financial operations should also take into account the various normal and customary adjustments associated with the payment ecosystem. It is necessary for the PF to validate the collection and disbursement of appropriate fees, adjustments, assessments and interchange for submerchants and at the portfolio level on a daily and monthly basis.

Examples of submerchant adjustments include:

- ACH rejects (by reason code)
  - Fees
  - Submerchant settlement
- Diverts/Reserves/Holds
  - Submerchant bankruptcies/liens/garnishments
  - Suspect submerchant transactions
  - Cash advance remittances to submerchant lenders
  - Rolling and other submerchant reserves. Note: In all cases, reserved funds (see Section 4.15) are held by the acquirer with release request/approval necessary prior to release of funds to the submerchant by the PF.
  - Adjustments/Miscellaneous Items
  - Chargebacks
  - Equipment
  - Fees/fines

Daily and monthly guidelines should be maintained along with supporting submerchant records and documentation. These records will assist with the PF's financial and acquirer audits as they detail the procedures used by the PF to manage and reconcile the submerchant portfolio. The PFs settlement oversight and reconciliation practice should also include procedures that address the ancillary items that can impact submerchant settlement and the financial performance of the PF.

Some examples of these practices include:

- ACH write-offs – timing/escheatment
- Risk write-offs – timing
- Collections – timing/recovery
- Refunds: It is suggested that PFs track refund type by specific GL to determine the financial effect of each reason associated with refunds to submerchant. These operating results prove very beneficial in measuring both submer-

chant and PF staff behaviors and the resulting exposure to the PF.

- Submerchant reserve reporting (if applicable).

Monthly management reports should include the financial results/statistics that are gathered during the execution of the monthly write-off practice to ensure any potential financial exposure is adequately noticed and escalated to the appropriate parties. PFs should ensure that their reporting practices support any card scheme monthly, quarterly or annual reporting requirements.

## 6.2. Graduating Submerchants

A PF must continually monitor submerchant volumes and be prepared to graduate submerchants into a direct merchant relationship based on card scheme volume thresholds, Section 4.9. At attainment of the processing caps, a submerchant must progress to a direct merchant relationship due to its processing volume.

In these cases, a PF must ensure that the acquiring bank is a party to the contract. If the acquiring bank was on the original contract and all card scheme required elements were included, no further contract related action is necessary. If the acquiring bank was not included, then the PF must re-contract with the submerchant entering into a direct or tri-party relationship with the acquiring bank. It is imperative that PFs underwriting and risk monitoring practices take these card scheme volume thresholds into consideration to ensure compliance and avoid unnecessary risk or exposure to fines or fees.

Please note that when a submerchant graduates based on Visa's requirements, the overall settlement flow may continue through the PF. However, when the graduation is based on MasterCard's requirements, the settlement must go directly from the acquiring bank to the merchant (previously known as the submerchant).

PFs should refer to the ETA Guidelines for Merchant and ISO Underwriting and Risk Monitoring published January 2016 for the best practices on direct merchant on boarding, underwriting and risk monitoring.

## 7. Guidance on Transaction Receipt, Authorization Request, Clearing, Chargeback, Representation Records and Billing Descriptor Requirements

There are certain card scheme requirements that a PF must adhere to concerning naming and identification conventions for submerchants to ensure descriptors and dynamic MCC requirements are met at the prescribed hierarchy.

To ensure submerchants are appropriately identified to cardholders, specific naming conventions must appear on consumer billing statements and receipts. Prominently identifying the submerchant rather than the PF in the appropriate name fields ensures transaction recognition, appropriate escalation path for customer support and fewer cardholder disputes.

Both PFs and their submerchants must be identifiable and recognizable in a transparent fashion to the cardholder of record. Proper use of descriptors and identifiers result in fewer consumer chargebacks, which protects the PF, the card schemes and the overall payment landscape from reputation damage and risk loss.

Both the PF and the submerchant must be identified in the various records associated with the submerchant's transaction processing, clearing and reporting. PFs must configure and administer systems to support, at a minimum, the following unique identifiers in the formats specified by the card scheme:

- Transaction authorization and settlement records
- Descriptors
- Receipts
- Billing statements

Note that all transaction records must also include the designation of the MCC appropriate for the business type of the submerchant, not the PF. MasterCard requires to further identify the relationship between the PF and submerchant, a specific ID that matches the company ID assigned the PF during registration by MasterCard. This unique PF identifier (submerchant ID field) is utilized as a cross reference to the submerchant records. American Express also has some specific PF requirements for reporting and submerchant identification. PFs should ensure their policies and practices incorporate the rules and regulations of each card scheme as appropriate.

Compliance with these requirements is necessary to avoid fines, assessments and reputational damage. Due to the complexity of certain technical specifications and changing legal terrain, PFs should rely on card scheme rules and expert opinion to ensure compliance and legality.

## 8. Conclusion

The PF guidelines included in this document are the result of a collaborative effort among ETA members based on their recognition of the need for an educational initiative for ETA member payment facilitators regarding effective tools for protecting the consumer, submerchants, and the card acceptance ecosystem. These guidelines are not exhaustive but may be helpful to ETA member payment facilitators of all sizes and at all levels of organizational complexity in underwriting, monitoring and managing submerchants and ISOs at varying levels of risk exposure.

ETA member payment facilitators should provide feedback regarding additional considerations for future versions of these guidelines and ongoing educational efforts to keep all ETA member payment facilitators informed of emerging opportunities based on advances in technology and the effects those opportunities have on underwriting and risk management practices.

ETA member payment facilitators have the latitude to determine the methods to perform gap analysis and implement recommendations as best fits the complexity of their individual organizations so long as the minimum requirements of the card schemes, their bank and governing regulatory authorities are met. Once an ETA member payment facilitator has gone through an internal gap analysis and implemented the guidelines or other risk mitigation tools as appropriate for their individual business needs, an agile business approach as defined throughout this document can make future incorporation of additional, newly defined effective business practices more manageable.

## Exhibit A

### Quick Reference Guide to Applicable Laws and Regulations

CARD SCHEMES	
Visa Core Rules and Visa Product and Service Rules	<a href="https://usa.visa.com/dam/VCOM/download/about-visa/15-April-2015-Visa-Rules-Public.pdf">https://usa.visa.com/dam/VCOM/download/about-visa/15-April-2015-Visa-Rules-Public.pdf</a>
MasterCard Rules	<a href="https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html">https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html</a>
American Express	<a href="https://www209.americanexpress.com/merchant/services/en_US/merchant-regulations">https://www209.americanexpress.com/merchant/services/en_US/merchant-regulations</a>
Payment Card Industry Data Security Standards (PCIDSS)	<a href="https://www.pcisecuritystandards.org/document_library?category=pcidss&amp;document=pci_dss">https://www.pcisecuritystandards.org/document_library?category=pcidss&amp;document=pci_dss</a>
US DEPARTMENT OF TREASURY	
Bank Secrecy Act (BSA)/ Anti-Money Laundering Laws (AML)	<a href="https://www.fincen.gov/statutes_regs/bsa/">https://www.fincen.gov/statutes_regs/bsa/</a>
US DEPARTMENT OF JUSTICE	
U.S. Patriot Act	<a href="https://www.fincen.gov/statutes_regs/patriot/">https://www.fincen.gov/statutes_regs/patriot/</a>
CONSUMER FINANCIAL PROTECTION BUREAU (CFBP) LAWS AND REGULATIONS	
Unfair, Deceptive, or Abusive Acts or Practices (UDAAP)	<a href="http://www.dfi.wa.gov/documents/credit-unions/compliance-manual/udaap-overview.pdf">http://www.dfi.wa.gov/documents/credit-unions/compliance-manual/udaap-overview.pdf</a>
FEDERAL TRADE COMMISSION	
The Federal Trade Commission (FTC) Act and FTC Bureau of Consumer Protection	<a href="https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act">https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act</a>
	<a href="https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection">https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection</a>
The FTC Fair Credit Reporting Act (FCRA)	<a href="https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act">https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act</a>
The FTC Dot Com Disclosure Guidelines	<a href="https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf">https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf</a>
FTC Guidelines for Online Negative Option Marketing	<a href="https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf">https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf</a>
	<a href="https://www.ftc.gov/news-events/press-releases/2014/07/ftc-will-keep-negative-option-rule-its-current-form">https://www.ftc.gov/news-events/press-releases/2014/07/ftc-will-keep-negative-option-rule-its-current-form</a>
The FTC Franchise and Business Opportunities Rule	<a href="https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/franchise-rule">https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/franchise-rule</a>
Red Flags Rule	<a href="https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule">https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule</a>
Telemarketing Sales Rule (TSR)	<a href="https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/telemarketing-sales-rule">https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/telemarketing-sales-rule</a>
Telephone Order Merchandise Trade Regulation Rule	<a href="https://www.ftc.gov/news-events/press-releases/2014/09/ftc-issues-final-amendments-mail-or-telephone-order-merchandise">https://www.ftc.gov/news-events/press-releases/2014/09/ftc-issues-final-amendments-mail-or-telephone-order-merchandise</a>
	<a href="https://www.ftc.gov/tips-advice/business-center/guidance/business-guide-ftcs-mail-internet-or-telephone-order">https://www.ftc.gov/tips-advice/business-center/guidance/business-guide-ftcs-mail-internet-or-telephone-order</a>
The Restore Online Shopper's Confidence Act	<a href="https://www.ftc.gov/enforcement/statutes/restore-online-shoppers-confidence-act">https://www.ftc.gov/enforcement/statutes/restore-online-shoppers-confidence-act</a>

<b>FEDERAL COMMUNICATIONS COMMISSION</b>	
Telephone Consumer Protection Act (TCPA)	<a href="https://transition.fcc.gov/cgb/policy/TCPA-Rules.pdf">https://transition.fcc.gov/cgb/policy/TCPA-Rules.pdf</a>
<b>OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)</b>	
Advisory on Merchant Processing	<a href="http://www.occ.treas.gov/publications/publications-by-type/comptrollers-handbook/pub-ch-merchant-processing.pdf">http://www.occ.treas.gov/publications/publications-by-type/comptrollers-handbook/pub-ch-merchant-processing.pdf</a>
Risk Management Guidance	<a href="http://www.occ.treas.gov/news-issuances/bulletins/2015/bulletin-2015-48.html">http://www.occ.treas.gov/news-issuances/bulletins/2015/bulletin-2015-48.html</a>
Third-Party Relationships Risk Management Guidance	<a href="http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html">http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html</a>
<b>FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)</b>	
Guidance on Payment Processor Relationships, Risk Management Examination Manual for Credit Card Activities	<a href="https://www.fdic.gov/news/news/financial/2008/fil08127a.html">https://www.fdic.gov/news/news/financial/2008/fil08127a.html</a>
	<a href="https://www.fdic.gov/regulations/examinations/credit_card/">https://www.fdic.gov/regulations/examinations/credit_card/</a>
	<a href="https://www.fdic.gov/news/news/financial/2013/fil13043.html">https://www.fdic.gov/news/news/financial/2013/fil13043.html</a>
Supervisory Approach to Payment Processing Relationships with Merchant Customers That Engage in Higher-Risk Activities	
Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA)	<a href="https://www.fdic.gov/news/news/financial/2010/fil10035a.pdf">https://www.fdic.gov/news/news/financial/2010/fil10035a.pdf</a>
<b>BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES</b>	
Laws, Regulations and Rulings	<a href="https://www.atf.gov/rules-and-regulations/rules-and-regulations-library">https://www.atf.gov/rules-and-regulations/rules-and-regulations-library</a>
<b>IRS</b>	
Backup Withholding	<a href="https://www.irs.gov/taxtopics/tc307.html">https://www.irs.gov/taxtopics/tc307.html</a>
1099	<a href="https://www.irs.gov/pub/irs-pdf/i1099k.pdf">https://www.irs.gov/pub/irs-pdf/i1099k.pdf</a>

## Exhibit B

### Website Basic Review Checklist

All website pages must be captured and stored with the submerchant file either in paper or electronically.

Submerchant Name: \_\_\_\_\_

URL: \_\_\_\_\_

Domain Name Owner Captured From Whois: \_\_\_\_\_

Server Location: \_\_\_\_\_

Type of Product Sold: \_\_\_\_\_

Customer Support contact information: \_\_\_\_\_

Phone: \_\_\_\_\_ Email: \_\_\_\_\_

Address: \_\_\_\_\_

#### Terms and Conditions:

Does corporation name match application name?  Yes  No

Negative option billing:  Yes  No

Are charges listed other than the ONE on the purchase page?  Yes  No

Membership of any type:  Yes  No

Privacy Policy:  Yes  No

Data Share:  Yes  No

Shipping Policy: \_\_\_\_\_

Refund Policy: \_\_\_\_\_

Currency in U.S. Dollars:  Yes  No

Secure Processing:  Yes  No

Initials of Person Performing Review: \_\_\_\_\_ Date of Review: \_\_\_\_\_

## Exhibit C

### Quick Reference Guide to Online Review Resources

Resource Name	Link	Description
Superpages.com	<a href="http://www.superpages.com">http://www.superpages.com</a>	Address/Phone Reverse Search
MasterCard Online (TMF search)	<a href="https://www.mastercardconnect.com/pu">https://www.mastercardconnect.com/pu</a>	Used to access MasterCard
	<a href="blic/extranet/login/workspace.html">blic/extranet/login/workspace.html</a>	Match/TMF Search
Domain/URL/Whois Lookup	<a href="http://whois.domaintools.com/">http://whois.domaintools.com/</a>	URL/Domain registration search used to verify who registered a website
People Search	<a href="http://www.pipl.com/">http://www.pipl.com/</a>	Address/Phone Reverse Search
Business Filings	<a href="http://www.llrx.com/columns/roundup29.htm">http://www.llrx.com/columns/roundup29.htm</a>	Used to access state corporation records
Texas State Site	<a href="http://ecpa.cpa.state.tx.us/coa/Index.html">http://ecpa.cpa.state.tx.us/coa/Index.html</a>	Used to access state corporation records
Nonprofit Organization Lookup	<a href="http://www.melissadata.com/lookups/np.asp">http://www.melissadata.com/lookups/np.asp</a>	Reverse search to verify non profit status
Better Business Bureau	<a href="http://www.bbb.org/us/Find-Business-Reviews/">http://www.bbb.org/us/Find-Business-Reviews/</a>	Access to BBB reports – used to view customer comments for a merchant
Federal Reserve Routing # Directory	<a href="http://www.fededirectory.frb.org/searchACH.cfm">http://www.fededirectory.frb.org/searchACH.cfm</a>	Used to verify routing numbers provided on applications
EBay Member Search	<a href="http://shop.ebay.com/ebayadvsearch/W0QQadvZ1QQsofindtypeZ25?rdc=1">http://shop.ebay.com/ebayadvsearch/W0QQadvZ1QQsofindtypeZ25?rdc=1</a>	Used to verify Ebay member/seller ratings and view customer comments
Rip-off Report	<a href="http://www.riporffreport.com/">http://www.riporffreport.com/</a>	Used to view customer comments for a merchant
Alexa	<a href="http://www.alexa.com/">http://www.alexa.com/</a>	Website traffic and information. Global ranking/ time on site/ website visits by country
Scam.com	<a href="http://scam.com/">http://scam.com/</a>	Works as a message board regarding various fraud merchants and schemes
Network solutions	<a href="http://www.networksolutions.com/whois/index.jsp">http://www.networksolutions.com/whois/index.jsp</a>	Gives the name of the person or company who own the rights to the website. IP/ physical address is also disclosed.
Wayback Machine	<a href="http://archive.org/web/web.php">http://archive.org/web/web.php</a>	Will give you the exact look of a website during a specific period of time.
IC3	<a href="http://www.ic3.gov/media/default.aspx">http://www.ic3.gov/media/default.aspx</a>	Works as a message board regarding various fraud merchants and schemes. Explains how the schemes work.
Bureau of Consumer Protection Business Center	<a href="http://business.ftc.gov/documents/bus28-advertising-and-marketing-internet-rules-road">http://business.ftc.gov/documents/bus28-advertising-and-marketing-internet-rules-road</a>	Is a legal resource to ensure compliance with laws and regulations in many industries.
Salty droid	<a href="http://saltydroid.info/">http://saltydroid.info/</a>	An opinion blog reviewing internet marketers.

## Exhibit C

### Sample Periodic Review

Date: 11/11/13

PRIN – Agent group

Fixed/rolling reserve MSI: \$\$,\$\$\$,\$\$

5%/10%/20% reserve

Merchant: Name

Signer: Name

Top 250

Approved for \$\_\_\_K/month

#### PROCESSING SNAPSHOT

--Chart of current YTD and last year processing - including # of sales/returns/CBs and volume of sales/returns/CBs. Also included is CB ratio and return ratio

#### PROCESSING SNAPSHOT

-

Ex:

	MTD			YTD			2012		
	Tickets	Vol	Avg ticket	Tickets	Vol	Avg ticket	Tickets	Vol	Avg ticket
Sales	22598	\$ 639,772	\$ 28	74237	\$ 2,047,162	\$ 28	0	\$ -	#DIV/0!
Returns	145	\$ 5,745	\$ 40	861	\$ 31,749	\$ 37	0	\$ -	#DIV/0!
Return %	0.64%	0.90%		1.16%	1.55%		#DIV/0!	#DIV/0!	
Net Sales	22453	\$ 634,027	\$ 28	73376	\$ 2,015,413	\$ 27	0	\$ -	#DIV/0!
Chargebacks	3	\$ 58	\$ 19	19	\$ 550	\$ 29	0	\$ -	#DIV/0!
CB %	0.01%	0.01%		0.03%	0.03%		#DIV/0!	#DIV/0!	
YTD Profit	\$ 18,564								
YTD Profit margin	132	Basis Points							
LY Profit	\$ -								
LY Profit margin	#DIV/0!	Basis Points							

Boarded Date

#### OVERVIEW

-Summary of business, what they are selling, business practices, etc.

##### is a daily deal website selling primarily jewelry and accessories. All items on site at time of review were under \$50. I found #####, Inc. on BBB, which has an F rating. Same address and signer are listed on site, and complaints point to #####. Issues revolve around delivery complaints (based on volume of sales, makes sense fulfillment could be an issue). BBB shows signer as the owner, business started in April 2011, and BBB opened in February 2012. Searches pull up some affiliate blogs directing traffic as well as some complaints.

Website links:

## Exhibit E

### 6 Month Trending

Sales	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
Sales #						
Credit \$						
Credit #						
CB \$						
CB #						
Credit %	# refunds/# sales					
CB %	# chargebacks/# sales					
ACH Reject Amount						
Reserve Amount						

## Exhibit F

### Quick Reference Guide

### Website Meta Tag Review



### Advertisements



When you hover your mouse cursor over different areas of a webpage, the associated URL will pop up at the bottom of your screen:



### Meta Tags:

Meta tags are hidden to the naked eye but exist within the source code of a Web page and can define what the website is about.

A page's title, description and keyword tags generally appear at the top of a Web page's HTML code. You can typically find a page's meta tags by right-clicking on the page and selecting "View source."