FINANCIAL COALITION AGAINST CHILD PORNOGRAPHY

Internet Merchant Acquisition and Monitoring Best Practices for the Prevention and Detection of Commercial Child Pornography*

Background

The Financial Coalition Against Child Pornography ("Coalition") was formed in 2006 to address the alarming growth of commercial child pornography over the Internet. Its members include leaders in the banking and payments industries, as well as Internet services companies. One of the Coalition's charters is to prevent child pornography merchants from entering the payments system and establishing merchant accounts with members of the Coalition. As a first step, the Prevention Working Group of the Coalition undertook a review of the methods the banking and payments industries employ to scrutinize on-line merchants in order to identify best practices associated with stopping the distribution and sale of child pornography over the Internet.

This document contains a compilation of methods that some Coalition members have used in their application and verification process, and thereafter, to detect child pornographers and prevent them from establishing or maintaining merchant accounts. These methods are being shared in an effort to assist other Coalition members in evaluating their respective procedures for detecting commercial child pornographers and preventing commercial child pornographers from obtaining access to services offered by Coalition members.

Given the increasing sophistication level of these crimes, the Coalition recognizes the challenges involved in meeting its goal of preventing all commercial child pornographers from obtaining access to our systems.

By utilizing these methods, or appropriate variations thereof, Coalition members can conduct comprehensive risk assessments of entities applying to use their services. The Coalition also recognizes that each Coalition member has different business models and products, and not all of these methods may be applicable to, or equally effective for, all Coalition members. The Coalition also realizes that rapid advances in technology or other changes may require modification to these methods. We encourage the Coalition members to use the strategies below or to adopt modified ones as appropriate.

It is important to note that the practices, methods, and red flags contained in this document are only suggestions. It is the responsibility of each Coalition member to establish its own merchant acquisition policies and procedures appropriate to its respective business models, risk assessments, internal policies, and/or regulatory oversight.

Methods for Detection and Prevention

Effective due diligence is essential to assess the legitimacy and viability of merchants who desire access to join the payments system. This is especially true of merchants who are doing business over the Internet as it can be challenging to properly identify a merchant and effectively control the methods and sales channels a merchant may utilize to support its business. The following sections offer examples of best practices that can be employed during merchant acquisition and monitoring to prevent/detect on-line merchants involved in commercial child pornography.

The Merchant Application

The Merchant Application is the foundation of a financial institution's relationship with a merchant. It is an effective tool for collecting the merchant's credit qualifications for verification and assessing its potential risk for fraud. As part of the initial merchant review, it is important to follow generally accepted "know your customer" procedures and guidelines appropriate to the Coalition member's business model/risk assessments/regulatory oversight. The merchant application should be comprehensive enough to gather relevant background information on the merchant, its business model, products or services it offers, operations, locations, principals and other key personnel, which potentially may also include the items listed below. Each Coalition member should, however, employ its own due diligence process based on its own internal policies, regulatory requirements, and procedures. Additionally, each Coalition member needs to take into account the impact of local laws on the acquisition process when operating internationally. The best practices set forth in this document focus on some of the methods that Coalition members use when specifically acquiring Internet merchants, which can be used to supplement members' standard practices (when appropriate).

Merchant Business Background

- Merchant history: Obtain the merchant's authorization to research its background, including credit, banking, financial history and history of card acceptance (merchant statements). Ask the merchant to supply information for any other businesses it currently owns or operates, or has owned in the past. Ask if the merchant and/or any other principals involved have a prior merchant relationship with acquiring banks. If yes, request bankcard statements for several months of activity. If another Acquirer previously terminated the merchant, note the reason for termination on the merchant's application.

- Doing-Business-As (DBA) or trade name: Both the DBA name and the legal/trade name should be disclosed on the application. Some merchants may conduct their daily business activities under one name and apply for legal registration under a different name. If the names are materially different, it is important to know both names and the reasons supporting any material differences. Inquire into the Better Business Bureau to obtain a record of performance for the DBA, legal name, phone number and website URL.

- Legal Structure: Inquire about the legal form of the merchant's business. For example, is the merchant a partnership, sole proprietorship, or corporation? Verify business licenses; professional licenses; or a corporate charter, articles of incorporation or similar documents.

Check for consistency in the information and compare to all other application information. Remember that publicly available documents such as articles of incorporation are easy to obtain and to fabricate, so certain circumstances may favor verifying non-public records, such as driver's licenses, passports, telephone or utilities bills, tax returns, etc. Please be cognizant of data security and privacy issues with regards to this type of information outside of what is required for verification purposes. Verify the merchant's business license number or any other license or registration numbers that may be required to own and/or operate a business. Perform a search with the appropriate business bureaus to verify that the merchant owns or operates a legitimate business.

- Independently confirm the business bank account. Compare the account number to the one noted on the application to ensure a match. Ensure that the name on the bank account the merchant wishes to deposit settlement proceeds into matches the legal name of the applicant and/or agreement holder.

- Consider asking the merchant whether it has the ability to restricts sales, specifically e-Commerce sales, by IP address for specific countries and, if so, why. (For example, in the Regpay case, the child pornographers blocked transactions from certain countries including Belarus (where they were located) and Latvia (where they banked), in an effort to restrict law enforcement from conducting test transactions.)

Merchant Business Operations

- Consider asking for information at the initial application regarding the merchant's sales volume, processing activity, billing/shipping methods and product or services it offers to better understand the merchant's operations. Additionally, this information can be used to compare to actual processing metrics, once the merchant is live to determine if the merchant's business activity has changed, which can be an early warning sign for illegal activity and/or processing in a manner for which the merchant is not approved.

  Information requested on the application might include some of the following:

  - Projected or actual annual sales volume;
  - Projected or actual annual sales that are credit and debit card related;
  - Projected or actual chargeback volume including count and % of sales;
  - Projected or actual refund volume including % of sales;
  - Percentage of sales by mail order, telephone order, or Internet;
  - Period between the time a consumer is billed for a product or service and actual shipment of those goods;
  - Guarantees and ongoing services (copies of consumer contracts could be requested);
  - Product or service offered by the merchant;
  - Marketing method of product or service, % that is recurring billing or subscription based;
  - Marketing materials of merchant (printed brochures, web pages, mailers, etc);
  - Copy of the posted refund or cancellation policy and card acceptance disclosures; and
  - Disclosure of all sales channels, including any and all URLs if e-Commerce related.

- Cards honored. When possible, identify what other (if any) bank or travel and entertainment cards the merchant honors and the name of the acquiring institution.

Merchant Ownership Information / Principal(s) Information

- Ask the merchant for the full legal name, address, Social Security Number or Tax ID Number (or similar identification number) and telephone number for every principal and/or corporate owner. Local laws may affect the information that can be obtained.

- Obtain the percentage of ownership held by each principal and how long each of the current principals has had an ownership interest in the business. Consider requesting a guarantee from the officers of the corporation.

The Application Process for Internet Merchants

Some Coalition members use a separate application and establish a set of credit/risk underwriting criteria for all merchants establishing an e-Commerce presence. Consider using this practice when the applicant is an existing merchant that wants to add a website or Internet presence or a new merchant that wants to apply for services. This practice can help facilitate the special risk assessment actions related to card-not-present (CNP) volume and the risks inherent in that business model. It can also allow for merchant business name and site content verification, as well as ensure that the correct business name is displayed on cardholder statements. In addition, a separate application form provides an easier way to track and report e-Commerce application volume. Consider having separate tiers (i.e. low risk, moderate, high risk, etc.) for Internet merchants based on the product or service they offer with varying levels of underwriting criteria based on the level of risk.

Consider a separate policy for any "Third Party" merchant processing, which may include any Internet Payment Service Providers (IPSP's), Independent Sales Organizations (ISO's), Member Service Providers (MSP's), Product Fulfillment Vendors and Third Party Providers (TPP's). The associated policies and underwriting procedures should require additional due diligence into the Third Party itself, including some of the following: processing history, registration status, financial wherewithal, history and background of principals, types of products and/or services offered. Additionally, there should be visibility and enforceability through to the underlying merchants in that Third Party program, which could include underwriting screening/sampling, ongoing monitoring and review, termination rights, ability to hold/suspend funding, etc.

Note: Special consideration and due diligence should be given to any merchant that operates in an aggregator fashion, specifically any "Internet mall" merchants or web hosting firms.

- Consider gathering additional application information for all CNP merchants. Additional application information could include: detailed business plans; samples of merchandise; and/or copies of all relevant marketing materials, including catalogs, brochures, telemarketing scripts, website screen shots and print and broadcast advertisements. (Please ensure that appropriate privacy regulations are followed with regard to the retention of this information.)

- Risk exposure can be lowered by taking a few extra steps during the Internet merchant application process. Consider gathering additional information from Internet merchants, which could include: Universal Resource Locator (URL), also known as the website address (e.g., www.merchant.com) and Internet Protocol (IP) server address for the merchant website. By collecting this information, an acquirer is able to review the actual website and confirm that the Internet merchant is conducting the business as described on its application. You can also identify other URL's that reside on the server IP address.

- Secure contact details for the website hosting service. Contact the hosting service as another source to verify that the Internet merchant maintains a legitimate business.

Underwriting and Verification of Internet Merchants

In addition to a robust application process, the Coalition suggests the following best practices/methods for underwriting and verification of Internet merchants. As noted above, not every practice/method below will be applicable to all business models. Coalition members should use their best judgment to assess the risk presented by an Internet merchant and respond accordingly.

- Review the application and all additional information and, if necessary, request additional business financials and/or a personal guaranty from the principal(s).

- Verify that the telephone number listed is a bona fide business number. If the telephone number listed is an extension of a large business, call the main number to confirm the validity of the application.

- Verify that the telephone number listed reaches the individual contact person/employee.

- Verify the receipt and authenticity of backup documentation (when required) utilizing any appropriate third party resources.

- Verify that the individual contact person is employed by or represents the merchant entity.

- It is suggested that Coalition members run background and reference checks for merchant principal(s), partners, or owners using personal and business credit reports to better assess the risk and make a more informed decision. Additionally, obtain bank and trade references as appropriate to validate that the business is legitimate and in good standing with its creditors. Compare the address and phone number on the merchant application to the credit report to search for a match. If you cannot find a clear match for the merchant, attempt to call the merchant at the phone number listed on the credit report.

- Consider running an Internet search on the merchant to further inquire and validate the merchant's existence and business purpose. Also compare the information returned in this manner to make sure it is consistent with the other search results and the application itself.

Any material inconsistencies in this information should be questioned and investigated to the satisfaction of the underwriter.

- Submit an inquiry to the Issuers' Clearinghouse Service (ICS) to determine if Visa and MasterCard Issuers have reported:

  - Fraud or excessive credit card applications;
  - The filing of previous bankruptcies; or
  - The use of negative data on an application (e.g., a deceased principal's Social Security number, address, or phone, etc.)

- Inquire whether the merchant or its principals, owners or partners are listed on the MATCH (Member Alert to Control High Risk) file.

- Screen new merchant applicants against lists maintained by the Office of Foreign Assets Control of the US Department of the Treasury.

- In those instances when a merchant requests to open more than one account, determine the merchant's business rationale for operating under multiple accounts.

- Depending upon the Coalition member's risk assessment of a merchant, it may be advisable to visit a merchant's business location and meet with the business principal(s). When this is done, review with the principals the merchant's business model and complete an inspection of the premises, inventory, systems and merchant facilities to understand the type and nature of the merchant's business and reasonably ensure the merchant is not engaging in the distribution of child pornography. Third party entities can also be helpful in conducting this service depending on available resources. When it is deemed not feasible or necessary to visit a merchant's premises, members can interview the principals by telephone and view the premises using readily available satellite imaging tools. Utilizing these tools is a cost-effective way to determine if a location provided by the merchant is indeed a business office or similar facility, as opposed to a private residence. In addition, consider random or auditing-type site visits of merchants who warrant such monitoring.

- Initiate a comprehensive scan and review of the merchant's website and all related links from that website to properly assess risk and ensure that the merchant is engaging in a legal enterprise. As warranted, execute further searches through proprietary and third party tools to ensure that the merchant is not associated or connected with other websites that are not listed on the initial application.

- Consider underwriting standards that stipulate that the following information appear on the merchant's website:

  - Customer service number (toll free preferably);
  - E-mail address to contact the merchant;
  - Statement on security controls;
  - Delivery methods and timing;

- Refund and return policies;
- Privacy statements (permissible uses of customer information); and
- If an adult merchant, ensure statement 2257 is present and appropriately displayed.

- Use Internet merchant rating services to obtain additional information about existing Internet merchants. Consider utilizing appropriate third party services to verify the registered owner of the URL to see that it properly relates to or matches the merchant applicant.

- Consider copying and retaining the merchant website source code for periodic reviews. By retaining prints or saving the merchant's original website content for its primary pages (e.g., the original HTML code), comparisons can periodically be made between it and the current website. This offers an easy way to identify significant changes in the merchant's business (e.g., changes in products being sold or key affiliations to other websites).

- Coalition members may want to establish criteria for reviewing applications from a merchant's other locations. These procedures may be abbreviated from the standard underwriting guidelines. Verification should ensure that the type of business is similar to the existing location and that the merchant owns the additional locations. Examples of actions that could support this practice are as follows:

  - Obtain a summary application for any new sales outlet/URL or additional location for any existing merchant relationship.
  - Review all marketing material of the new outlet/location to determine the additional risk, if any, this new sales channel will present to the relationship.
  - Understand the relationship between the new merchant and existing merchant if the new outlet/location is being set up by a separate legal entity that is related through common ownership (i.e., an affiliate or subsidiary). If so, investigate the validity of the new merchant utilizing sound underwriting practices, including a financial review. Additionally check the new merchant against the MATCH database.
  - If the new outlet/location is a new URL/website, conduct a website review in accordance with your existing site review policies and procedures. Ensure you review all related links to the website and check the domain ownership for consistency.
  - Obtain sales projections, methods of payment accepted, billing and return policies to re-assess the credit exposure of this new outlet/location and dimension the impact of this new exposure on the overall relationship.
  - Review your processing agreement/contract to ensure that additional documentation is not required (e.g., a contract addendum to any new parties to the agreement).

- Educate external sales agents to ensure that they are aware of the member's policies regarding signing new merchants and share red flag indicators associated with merchants involved in child pornography.

Red Flags

Additional scrutiny is recommended if any of the following becomes apparent:

- The trading address is a private residence rather than an office in a recognized business area. This could indicate that the validity of the business is questionable or lacks financial substance.

- The merchant website appears to act as an "Internet mall" and hosts products and services provided by a variety of sources. There are links on the merchant's website to other sites to which they may or may not be affiliated. This should raise a flag if the linkages do not make sense or represent merchant types that you do not sign.

- The principals appear to lack a clear understanding of the business.

- The address indicated on the credit report is a mail drop (e.g., Mailboxes, etc.) as opposed to a street address.

- The merchant uses a generic mail carrier for its e-mail address, as opposed to an e-mail address that routes to the merchant's website. Verify that a merchant's e-mail address is valid by sending a message to that address. If the message is returned as "undeliverable" or "bounced", that may require further investigation.

- Consider heightened scrutiny for a business established for fewer than 90 days. You can determine the date on which a domain name was created by reviewing its hosting and domain records.

- The merchant website is not yet "live" at the time of application. Consider approving and setting up the merchant contingent upon a live site review and/or holding all settlement proceeds until the site can be properly reviewed.

Monitoring

After a merchant has successfully been verified and has entered the payments system, monitor it on an ongoing basis.

New Merchants

- The first few months after signing a new account may be a time of heightened vigilance, depending upon your risk assessment of the new merchant. At the most extreme risk category, consider a more frequent review of merchant activity during the first two- to three-months. It is recommended that the frequency of the periodic review intervals be directly tied to the credit and risk rating assigned to that merchant based on both the financial profile of the merchant (credit) and industry risks associated with its business model, product lines and/or method of delivery of those products and services.

- During this time, consider flagging and investigating any variations or deviations in activity. Suspicious activity may include variations in deposit frequency, transaction volume (velocity), average ticket price (ATP) of each sale transaction, change in percentage/level of refunds and chargebacks and refunds to credit cards without any corresponding sales.

- In addition, tighter exception parameters for new merchants are recommended. This will result in a greater number of reviews for these new accounts and is a prudent risk management practice for the first three to six months of a merchant relationship.

Ongoing Monitoring

- On a going-forward basis, monitor merchants for suspicious activity. This may be done via a scoring system, which will "Queue" merchants for review based upon a variety of transaction parameters. If there is a significant increase or change in processing activity such as average ticket, monthly volume, authorization, or velocity, investigate those increases.

- Look for a lack of merchant activity. Maintaining an inactive merchant account on file may represent potentially significant exposure to fraud. If an account has been inactive for two to three months, it could simply mean the merchant went out of business, is a cyclical or seasonal business or signed with another Acquirer. On the other hand, an inactive account could signal the fraudulent diversion of the merchant's deposits to a bogus merchant account with another Acquirer. It is therefore advisable to establish exception monitoring to flag inactive accounts and follow up on inactive accounts with the merchant.

- Consider a system enhancement that places inactive merchants in a "funding hold" category. Inactive merchants that are placed in this category still have an open account but the flow of funds is frozen. When the merchant becomes active again and tries to process a transaction, it receives an e-mail requesting that they contact customer service.

Additional Steps for Internet Merchants

Listed below are additional steps that may be considered for Internet merchants. It is recommended that the level of financial and website review of Internet merchants be dependent on the level of risk assessed to that merchant.

- Consider the use of anonymous merchant shopper programs, particularly in the first several months after a merchant goes live with processing. Additionally, shopping programs are recommended on an ongoing basis for Internet merchants based on either a random sampling of the merchant base or when processing activity exceptions have occurred that could be construed as suspicious activity. These types of programs use anonymous individuals who shop with merchants to evaluate customer service, billing and shipping methods and to validate whether the merchant offers the products it has claimed it sells.

- Determine the length of time between funding a transaction and receipt of the product by the cardholder so you can include the dollar amount in your risk formula.

- Verify the number dialed-in from the terminal to process the transactions and further investigate this number via the Internet to make sure this information links to the proper site/content/product.

- Confirm what products are being sold on the website as well as investigate any linked website to that merchant to verify that no additional products/services are being processed through the merchant account. Continuously referencing back to the original application information and what the merchant was approved for is an integral part of this process and will highlight any new products or services that may alter the risk dynamics of the merchant.

- Perform word searches at the merchant's websites, for such words as: "sedation", "bestiality", and "lolita".

- Keep a comprehensive list of "adult merchants" that process on your systems (if permitted by your own policies) and routinely monitor these accounts. If you process any adult merchant transactions via an IPSP or other Third Party Processor, ensure that you have the contractual rights to conduct ongoing audits of those sites and consider including a provision for the rights to approve any and all website and links prior to that merchant going live.

- Cross-reference any known adult merchants with card information to provide "linkage" to potentially illegal merchants.

- Monitor merchant submissions through a fraud-based program to identify changes in submission patterns and patterns that are not consistent with a particular industry type. Companies can leverage various monitoring processes and other merchant contact points to identify and investigate circumstances or characteristics that are inconsistent with the recorded merchant details, e.g., industry type, charge volume, transaction size, etc.

- Use fraud control strategies designed to detect unusually sharp increases in merchant authorization requests and merchant deposits through daily or real-time transaction monitoring. Unusual spikes in transaction activity may indicate that a merchant is factoring or aggregating transactions on behalf of its associated content suppliers.

- Consider engaging a third party company that uses web crawling or spidering services to review entire merchant portfolios to help ensure that merchants are not involved in aggregation or processing transactions that are questionable or illegal.

# # #

***The Coalition and each of its members disclaims liability for the use of this document. Each Coalition member is responsible for establishing its own merchant acquisition policies and procedures appropriate to its business models, risk assessments, internal policies, and/or regulatory oversight. No warranties, including no implied warranties of merchantability or fitness for a particular purpose, are made herein.**