Internet Merchant Acquisition and Monitoring Sound Practices to Help Reduce the Proliferation of Commercial Child Pornography

March 2016

FINANCIAL COALITION AGAINST CHILD PORNOGRAPHY

CONTENTS

DISCLAIMER

This report ("Report") was created and written by volunteers on behalf of the Financial Coalition Against Child Pornography (FCACP) and represents the current views of the issues addressed as of the date of publication. The content of the Report is based on the individual input of the contributors, and does not necessarily reflect the opinions or policies of the companies at which the individuals work, nor of any of the FCACP member companies.

The Report is for informational purposes only and does not render legal, financial, business or other professional services or advice. This Report may not be correct, complete, and/or up-to-date, so recipients should use this Report only as a starting point for their own independent research. If legal advice or other expert or professional assistance is required, the services of a competent professional should be sought. **THE FCACP MAKES NO WARRANTIES, EXPRESSED, IMPLIED, OR STATUTORY, AS TO THE INFORMATION CONTAINED IN THIS REPORT.** The listing of an organization or entity herein does not imply any sort of endorsement by such organization or entity.

Complying with all applicable copyright laws is the responsibility of the recipient. The Report may be freely redistributed in its entirety at no charge provided that the Report is not modified in any way and any disclaimers, legal notices, including all copyright notices, are not removed. It may not be sold for profit or used in commercial documents without the written permission of the FCACP, which may be withheld in the FCACP's sole discretion.

BACKGROUND

Formed in 2006, the Financial Coalition Against Child Pornography (FCACP) is a cooperative initiative between the financial and Internet industries to help eradicate the proliferation of commercial child pornography. It is managed by the International Centre for Missing & Exploited Children® (ICMEC) and the National Center for Missing & Exploited Children® (NCMEC). FCACP members include leaders in the banking and payments industries, as well as the Internet industry. One of the FCACP's charters is to prevent child pornography merchants from entering the payments system and establishing merchant accounts with members of the FCACP. As a first step, the FCACP examined the methods used by the banking and payments industries when examining online merchants in an effort to identify sound practices to help disrupt the distribution and sale of online child pornography.

The Report describes methods used by some FCACP members in their application and verification process, and thereafter, to detect child pornography and prevent the establishment or maintenance of merchant accounts related to the commercial distribution and sale of child pornography. These methods are being shared in an effort to assist other FCACP members in evaluating their respective procedures to detect and prevent commercial child pornography offenders from obtaining access to services offered by FCACP members.

Given the increasing sophistication of the methods used to facilitate the sale and distribution of online child pornography, the FCACP recognizes the challenges involved in meeting its goal of preventing all commercial child pornography offenders from obtaining access to payments systems, and the necessity of remaining vigilant.

By utilizing these methods, or appropriate variations thereof, FCACP members can conduct comprehensive risk assessments of entities applying to use their services. Because FCACP members may employ different business models and products not all of these methods may be applicable to or equally effective for all FCACP members. Additionally, rapid advances in technology or other changes may require modification to these methods. We encourage the FCACP members to review the strategies listed below and determine their suitability for use or modification as appropriate.

The suggested practices, methods, and red flags described in the Report are provided for informational purposes only. It is the responsibility of each FCACP member to establish its own merchant acquisition policies and procedures appropriate to its respective business models, risk assessments, internal policies, and/or regulatory oversight.

The Report was initially released in 2007. Volunteer members of the FCACP have updated and expanded these sound practices.

ESTABLISHING A COMPANY'S POLICY OR TERMS OF USE

The foundation of a company's risk management program is its policy or terms of use. As it relates to the subject of this Report, the policy or terms of use must clearly articulate that the processing of payments for the distribution of child pornography will not be permitted. Any merchant doing so will be removed from the payments system.

MERCHANT ACQUISITION

Effective due diligence is essential to assess the legitimacy and viability of merchants who desire 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 sound practices that can be employed during the merchant acquisition and monitoring processes to prevent/detect online 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 FCACP's 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 and/or services it offers; operations; locations; principals and other key personnel. FCACP members should consider using the following criteria as part of the application process. Each FCACP member should, however, employ its own due diligence process based on its own internal policies, regulatory requirements, and procedures. Additionally, each FCACP member needs to take into account the impact of local laws on the acquisition process when operating internationally. The sound practices set forth in this Report focus on some of the methods that FCACP members use when specifically acquiring Internet merchants, which can be used to supplement members' standard practices as 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 or other similar business-vetting organizations to obtain a record of performance for the DBA, legal name, phone number and website Universal Resource Locator (URL).

- Legal Structure: Inquire about the legal structure of the merchant's business. For example, is the merchant a partnership, sole proprietorship, or corporation? Verify business and professional licenses, corporate charter, articles of incorporation, or similar business documents. Check for consistency in the information and compare the information to the submitted application. Remember that publicly-available documents such as articles of incorporation are easy to obtain and may contain false representations, so certain circumstances may favor verifying non-public records, such as driver's licenses, passports, telephone or utilities bills, tax returns, etc. FCACP members should first consider data security, legal and privacy issues prior to obtaining this type of additional information. 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.

- Business Bank Account: 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.

- Physical Site Survey: Consider utilizing a physical site survey process for high-risk merchant account types. This could be performed by a sales person or possibly a third party agency.

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. This information can later be used for comparison purposes to determine if the merchant's business activity has changed, which may 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 percentage of sales;
  - Projected or actual refund volume including percentage of sales;
  - Percentage of sales by mail order, telephone order, or Internet;
  - The use of affiliate programs or other unique commission structures (percentage of sales generated through affiliates);
  - 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, including percentage that is recurring billing or subscription based;
  - Marketing materials of merchant (printed brochures, web pages, social media 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.

- When possible, determine whether the merchant accepts other bank, travel, or entertainment cards and the name of the acquiring institution.

- Consider asking the merchant whether it has the ability to restrict sales, specifically e-commerce sales, by Internet Protocol (IP) address for specific countries and, if so, why. (For example, in the Regpay case, the commercial child pornography companies 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.) If the merchant will not supply the information requested, consider denying the application.

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. FCACP members should first seek legal advice concerning any laws which may affect the ability to obtain this type of information.

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

Application Process for Internet Merchants

- Consider having separate tiers (i.e., low, moderate, high, etc.) for Internet merchants based on the product or service they offer with varying levels of underwriting criteria, as well as approval authorities, based on the level of risk. Some FCACP 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 gathering additional application information for all CNP merchants, including detailed business plans, samples of merchandise and relevant marketing materials such as catalogs, brochures, telemarketing scripts, website screen shots, social media pages, and print and broadcast advertisements. FCACP should seek professional and/or legal advice concerning any privacy regulations related to the retention of this information.

- Consider asking high-risk e-commerce merchants whether they have further capabilities or policies to screen activity based on the service they provide. For example, cyberlockers which allow consumers to store pictures or other materials could be screened by the cyberlocker provider (the merchant) to ensure child pornography is not being stored in the lockers.

- 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 URLs and IP addresses. 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. The acquirer can also identify other URLs that reside on the server IP address. Further, performing "WhoIs" or reverse "WhoIs" checks can provide valuable insight into ownership or registering agents of the site.

Use of Third-Party Merchant Processing

It is very common in the card processing industry for illicit merchant relationships to be initiated by third parties. As such, consider a separate policy and program for any "third party" merchant processing, which may include any Payment Facilitators (PF'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 processing history, registration and financial status, history and background of principals, and types of products and/or services offered. Additionally, there should be visibility and enforceability through to the underlying merchants in that third-party program, including underwriting screening/sampling, ongoing monitoring and review, termination rights, and ability to hold/suspend funding. Details of such third party

programs can be found in section 6 of the ETA Guidelines Merchant-ISO-Underwriting-Risk-Monitoring.
http://www.electran.org/wp-content/uploads/ETA-Guidelines-Merchant-ISO-Underwriting-Risk-Monitoring-2014.pdf

Underwriting and Verification of Internet Merchants

In addition to a robust application process, FCACP suggests the following sound practices/methods for underwriting and verification of Internet merchants. As noted above, not every practice/method below will be applicable to all business models. FCACP 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 legitimate 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. Call the number and make note of how the phone is answered. Is the company mentioned in the greeting? A phone answered with just "hello" may require further inquiry.

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

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

- It is suggested that FCACP 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, its email address and phone number 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.

- 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 or principal requests to open more than one account, determine the merchant's business rationale for operating under multiple accounts. Search internal databases for multiple merchant accounts with different names that are operated by the same principals.

- Search internal databases for other applicants that have submitted the same websites as their own. If possible, consider using an internal negative database to track individuals or merchant entities who have performed prior illegal activity.

- Depending upon the FCACP 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. If a merchant's website has non-working (i.e., "dead") links, make further inquiries. A "dead" link can become active later, thereby providing a channel for selling illegal content. Additionally, look for "ghost" links by moving a mouse over blank or non-specific areas. Let the site sit open for a while and then move the mouse over the same areas to see if anything appears. 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: (If these items are missing, it may suggest the website is being set up as a front for underwriting purposes only.)

    - Customer service number (toll-free preferably);
    - Email address to contact the merchant (Is the email address similar to the name of the website? A generic email address may require additional follow-up);
    - 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.

- Review the merchant's Internet presence. Go at least 5 pages deep on search engine results and review other relevant social networking and related sites such as Yelp, Twitter, Foursquare, LinkedIn and Facebook.

- Review IP address to:
    - Ensure the location is consistent with the merchant;
    - Ensure it is not in a high-risk country (i.e., Eastern Bloc countries);
    - Ensure it is registered to the merchant or principal;
    - Assess the legitimacy of hosting company by using some of the same tools you would use to assess the legitimacy of the merchant;
        - Ensure open date is consistent with business open date.

- Review site registration. It has been the experience of some of the FCACP members that "bad sites" may use proxy registration services to hide their true ownership. For a fee, proxy registration services will hide a URL owner's information and instead list the name of the proxy service. While there may be a legitimate privacy-related reason for a legitimate merchant to use a proxy service, illegitimate entities/principals often use proxy services to hide their identify. There are third-party vendors who, for a fee, will provide additional information on URLs (i.e., change in ownership, address, emails, phone) or provide information on other URLs with similar registration information. FCACP members should review any other websites with similar registration information.

- Try to make a purchase via a secret shopping program. Does it work or identify any other red flags related to the billing descriptor or name of the merchant?

- 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). Utilize third-party vendors, that will for a fee, monitor on an ongoing basis websites for content.

- FCACP 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 this is the case, 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 to estimate 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 stability.

➢ 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.

➢ Prices are quoted in a currency different than that of the merchant's location.

➢ The merchant uses a generic mail carrier for its email address, as opposed to an email address that routes to the merchant's website. Verify that a merchant's email 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.

Initial Monitoring of 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, review 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 may indicate possible fraudulent diversion of the merchant's deposits. It is therefore advisable to establish exception monitoring to flag inactive accounts and follow up on them 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 email requesting that it contact customer service.

- As warranted, review chargeback media to understand what cardholder are indicating they are purchasing from the merchant. Are the product/services purchased consistent with what was listed on the application?

Additional Steps for Monitoring 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.

- It is recommended that website reviews of existing merchants should be done at least monthly to ensure content has not changed significantly.

- Identify websites that are not operable but where the merchant continues to process transactions.

- 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.

- Verify the IP address used to process transactions aligns with the geo location of the merchant or is not coming from a foreign IP entity.

- Confirm what products are being sold on the website as well as review 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.

- 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 a Payment Facilitator 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 websites 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.

- Recognize that certain merchant types may present higher risks in regards to child pornography. These may include:

    - Cyberlockers or file sharing services – where cardholders pay to store data, pictures, or other electronic items on third-party servers. While most cyberlockers/file sharing services may be legitimate, they may not have the policies, process or systems in place to monitor users who use the cyberlockers/file sharing services to store, share, transfer or profit from child pornography. FCACP members should carefully review and understand how these merchants detect and prevent illicit activity.
    - Internet malls or aggregators of other merchant transactions - these merchants process transactions on behalf other merchants. These are especially high risk because the acquirer generally does not have the same level of visibility into the underlying merchants. FCACP members should ensure that the aggregator has the systems, staffing, procedures and processes that are at least equal to that of the FCACP member.
    - Merchants utilizing affiliate programs whereby compensation or commissions are paid to third-party affiliates that help drive traffic to the merchant's website and help generate the sale of products or services (particularly when the merchant product or service is not tangible – such as downloadable software, website building, or consulting services). Illicit actors may use a legitimate merchant's affiliate marketing program to launder funds on behalf of an illicit website. FCACP members should understand the due diligence that the legitimate merchant conducts on its affiliate participants. Of particular concern are merchants who conduct limited due diligence on their affiliates and offer large and quick payouts to affiliates.

- Web-based advertising sites – merchants exclusively allowing the advertising of goods or services. These web-based classified ads may contain ads for illicit activity. FCACP members should review and understand the system and processes these entities have to detect and remove ads for illicit activity.
- Review sites – members pay for a service to read and post reviews of products or services, especially those regarding adult services.

CONCLUSION

The FCACP, in collaboration with ICMEC, NCMEC, and law enforcement, has made significant progress in the fight against commercial child pornography, as demonstrated by the significant drop in the number of unique commercial child pornography websites reported to NCMEC's CyberTipline®. At the same time the FCACP recognizes that it must remain vigilant to maintain that progress and to prevent child pornography merchants from entering the payments system. It is the FCACP's hope that this Report will be a useful resource to its members.

ADDITIONAL RESOURCES

Electronic Transactions Association Guidelines for Merchant ISO Underwriting and Risk Monitoring:
http://www.electran.org/wp-content/uploads/ETA-Guidelines-Merchant-ISO-Underwriting-Risk-Monitoring-2014.pdf

International Centre for Missing & Exploited Children (ICMEC) http://www.icmec.org/

National Center for Missing & Exploited Children (NCMEC):
http://www.missingkids.org/home

NCMEC's CyberTipline
http://www.missingkids.org/CyberTipline