ILLICIT FINANCE SPOTLIGHT SERIES
PRESENTED BY AML RIGHTSOURCE

THE CHILD PORNOGRAHPY CRIMINAL ENTERPRISE:

How the Financial Services Industry Can Help Disrupt

November 2017

Authored by:

Mici Chase, MS, CAMS
Associate, Financial Crimes Advisory
AML RightSource

Introduction

Crimes against children are heinous and known to be vilified even among the most notorious criminals, but these crimes are, unfortunately, also extremely profitable. The child pornography (CP) industry is a criminal business enterprise with far-reaching consequences for its victims. In a world of increasingly fast-paced, global, and anonymous transactional options, financial crimes professionals have a unique opportunity to see what others cannot, and a responsibility to aggressively research, report, and document child sexual exploitation. To this end, financial institutions (FIs) should develop targeted training programs, work collaboratively with other industries, align their reporting with law enforcement (LE) initiatives, and advocate for changes in Suspicious Activity Reporting (SAR) that will more effectively capture evolving trends pertaining to child pornography. In this article, we will explore how FIs can exceed regulatory standards, assist LE with money laundering prosecutions related to child pornography, cut the flow of funds to illicit criminal enterprises, and most importantly, help victims.

Who are the Victims, and Who are the Abusers/Consumers?

How can financial crimes professionals identify the primary parties involved in CP cases? The Internet Watch Foundation (IWF) serves as a great resource and an effective starting point. The IWF is a charity organization comprised of over 130 companies, including Google, Amazon, Facebook, and PayPal, with a mission to reduce CP material online and provide important statistics on new and existing CP trends. Its annual report from 2016 indicates that 53% of children identified in abusive images were 10 years old or younger; 45% were between the ages of 11 and 15; and 2% were two years old or younger. The vast majority of victims identified in these images (89%) were girls.[11]

There are several categories of abusers and consumers of child abuse images that your FI should be on the lookout for in CP investigations, the most common being pedophiles, situational abusers, and commercial providers. While pedophiles consistently prefer and seek out children for sexual activity, situational abusers occasionally involve children in sexual acts, given the right circumstances.[6] Commercial providers are individuals or criminal groups that produce and/or sell CP for the purpose of financial gain. Specificity, with regard to the identification of subjects who formulate the basis of your SARs, can be immensely beneficial to LE investigations and provide support for subsequent charges, arrests, and prosecutions involving those subjects.

Tactics, Techniques, and Procedures: What are the Crimes, and How are they Facilitated?

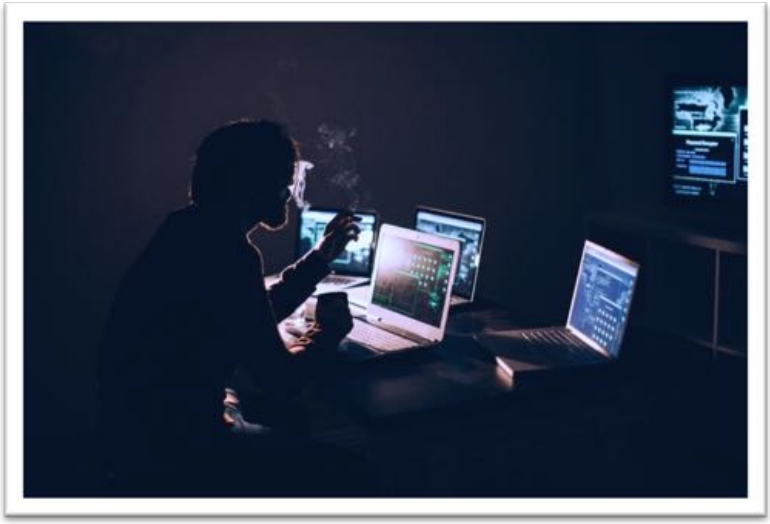
Identifying child pornography is not always a simple task, as the crime presents itself in various forms as illicit actors discover new tactics, techniques, and procedures (TTPs) to exploit in an effort to conceal their criminal endeavors.

IWF's annual report indicates that 28% of sexual abuse images identified show penetrative sexual activity, including rape or sexual torture, and 19% of images show non-penetrative

sexual activity.[11] Commercial CP can be obtained in a number of forms—some websites offer monthly or yearly membership access to content, including still photos, videos, live-stream material, and "self-produced" content created using webcams and subsequently shared online. Some websites require live-stream footage of the user with a victim as a criterion for website membership. Related material includes virtual child pornography or VCP (sexually explicit images of children that are entirely computer-generated, but realistic in appearance), partially-animated images, and sex dolls made to look like, or advertised as, pre-pubescent children.

Most CP websites offer two possible payment methods (some offer as many as five or six). Sites may offer traditional payment methods, such as payment with a credit or debit card, or a variety of alternative payment methods, such as internet, mobile, peer-2-peer (P2P) payments, prepaid cards, or digital currency.[5]

FIs should be aware that CP exists on both the surface and the dark web. According to IWF, 80% of websites containing graphic child sexual abuse images are still "Generic Top Level Domains," such as .com, or .net. As new domain suffixes are released, they are increasingly utilized for illicit purposes, the appeal for CP providers being that they are less-widely known. The number of pedophiles utilizing new domains rose by 258% since 2015.[11][4]



Commercial CP providers attempt to mask their activity through a number of tactics, a good example being pedophile codes. Pedophiles use certain code words for concealing and finding child sexual abuse images. Clues will sometimes be provided on online forums indicating where particular images are hidden on other websites. Providers also utilize disguised websites—websites which, when accessed directly through a browser, will display legal content, but when accessed through a specific digital pathway of links from other websites, will display illicit images. Legal adult pornography sites are often utilized for this purpose, putting legal viewers at risk of investigation. In 2016, 1,572 of these disguised websites were identified, a 112% increase since 2015.[11]

Interconnection with Other Crimes

CP is inherently linked to other crimes, namely child physical and/or sexual abuse, and is also often intertwined with a myriad of crimes, including child sexual exploitation, human trafficking/human smuggling (HT/HS), slavery, kidnapping, child sex tourism, and identity theft. While image-hosting sites serve as the primary forum for displaying CP, internet ad sites play a huge role in child sexual exploitation and HT/HS. An estimated 76% of transactions for sex with underage girls are processed through internet ads.[13] Ad sites typically have an Adult section with listings for escorts, erotic massage, strippers, phone sex operators, etc. These type of ads are inexpensive, easy to set up, and allow child sex traffickers to advertise a victim's services in multiple locations. Pictures of young children can be posted on advertising sites for the purpose of selling CP, selling their bodies for sex, or for selling the individuals outright.

Multiple financial crimes investigations have resulted from customer transactions made at Backpage.com, a classified advertising website that previously contained an Adult section, such as the one referenced above, containing subcategories for various sex work professions. These transactions were often in the hundreds, for small dollar amounts, and made multiple times a day on consecutive days. The aforementioned Adult section on Backpage.com was finally removed in January 2017 as a result of a US Senate Subcommittee report titled "Backpage.com's Knowing Facilitation of Online Sex Trafficking," a sub-section of which is titled "Backpage Knows Its Site Facilitates Child Sex Trafficking."[3] Backpage previously accepted several methods of payment for ads, but in 2015 the site lost all credit card processing agreements following continued issues with credit card processors, who were under pressure from LE to cease working with companies that allegedly allow or encourage prostitution. Bitcoin is currently the only remaining option for paid ads on Backpage.com.[12] As traditional payment options fall away due to increased pressure from LE, criminals turn to Bitcoin and other digital currencies due to their anonymity.

CP is also inherently linked to child sex tourism, or extraterritorial sexual exploitation of children, defined by the Department of Justice as "the act of traveling to a foreign country and engaging in sexual activity with a child in that country." Situational abusers may feel more comfortable committing these crimes in a foreign area due to greater anonymity, racism toward a particular group or culture, or due to the perception that these activities are actually helping impoverished children financially. Offenders can utilize the internet to plan travel specifically for this purpose.[6]

ECPAT International, a non-governmental organization exclusively dedicated to ending child sexual exploitation, published a study in 2016 which identified several North American cities as high-risk areas for child sex tourism, including Montreal, Atlanta, Las Vegas, and Washington D.C. The study identified the US and Canada as source countries for sex tourists who travel to other nations, as well as destination countries for sex tourists from other areas of the world, referencing business travelers, oil workers, and individuals passing through major transportation hubs. Reported offenses frequently occur along trucking routes and among temporary oilfield workers. Children from developing countries, poor or otherwise marginalized areas, and areas with ineffective LE are at greater risk.[8]

In a different vein, CP is also often linked to identity theft. CP sites sometimes advertise their material as a lure to steal personal identifying information (PII) from buyers at the time of purchase, such as credit card data, addresses, etc., with no intention of actually providing the desired pornography. The stolen data can be sold or used to make other illicit purchases. Some buyers will steal or purchase a stolen identity and use it to purchase CP, thereby remaining anonymous and potentially causing investigation into an entirely innocent party.[7]

The Role of National and International Organizations

National and international organizations have been instrumental in bringing together various members of the financial services industry to share information and resources in the fight against CP and related crimes. The Financial Coalition Against Child Pornography (FCACP) was established in the US in 2006 in response to a tremendous increase in CP material. The FCACP brought together a multitude of FIs, including American Express, HSBC North America, MasterCard, Visa, Standard Chartered and PayPal. The FCACP is instrumental in the discovery of new CP trends, authoring and issuing white papers, and developing guidance on CP and CP-related crimes for its member companies as proactive measures to ensure that the integrity of the financial system does not become compromised through illicit conduct.

The IWF also provides vital tools to help LE agencies and IWF member institutions detect and eliminate CP, including its list of pedophile code words, image hash list, and virtual currency alerts. The aforementioned list of pedophile code words is provided to IWF member companies each month to increase the detectability of CP activity. In December 2016, the list contained 442 code words associated with CP material. IWF also provides an image hash list, which assigns a unique code to child sexual abuse images, allowing the identification and removal of duplicate images. Virtual currency alerts are alerts issued to IWF member institutions whenever a Bitcoin wallet is identified as associated with child sexual abuse imagery. The number of commercial CP distributors accepting Bitcoin is still relatively low but has been on the increase since 2014. The virtual currency alerts allow IWF members to disrupt CP activity occurring in Bitcoin wallets.[11]

Protecting the Integrity of Your Financial Institution

Know Your Customer (KYC) Program

What measures can you implement to prevent CP from infiltrating your institution? While different institution types will require different measures, they should generally include a comprehensive KYC program with an emphasis on internet merchant vetting, appropriate transaction monitoring, and awareness of geographic areas at heightened risk for child sex crimes. The FCACP's white papers also detail best practices for avoiding and eliminating CP merchants and transactional activity. Establishment of an official written stance as part of an institution's enterprise-wide policies and procedures, prohibiting CP-related activity, is the critical first step. An institution's written policies should also clearly dictate whether any adult service merchants are permitted, and if so, they should receive heightened scrutiny prior to account opening, and throughout the lifetime of the account. As discussed, CP merchants often conceal their services behind legal adult content sites. Thus, a list of all adult merchants within an institution should be maintained and periodically reviewed.[10]

If adult merchants process transactions through a third-party payment processor (TPPP), the FCACP recommends securing contractual rights to conduct audits of those sites. In addition to adult service merchants, there are several other merchant types which present a heightened risk for CP. These include cyberlockers (file-storing and file-sharing services), internet malls (which host products and services provided by a variety of sources), merchants utilizing affiliate programs (where third parties are paid to help drive traffic to a merchant website), internet ad sites, and review sites (especially review sites regarding adult services).[10]

Merchant vetting is an extremely important component of KYC practices. In addition to baseline KYC procedures, internet merchants should be subject to Enhanced Due Diligence (EDD) standards of review. When a merchant applies for an account, a detailed review of the merchant website is critical. If the merchant website is not active at the time of application, an institution may want to consider approval only after a review of the functional site. An examination of the website should address a number of issues, including whether there are any linkages to other websites, and if so, whether the linkages are logical. The website should be checked for hidden links, which may be the same color as the website background, or otherwise obscured. Just as a prospective merchant must be a business type permitted by institution policy, so should any additional websites linked to the prospective merchant site. A reputable merchant is likely to have an email address connected with the merchant website, and if a generic email address is used, it should be verified as functional using a test email.[10]

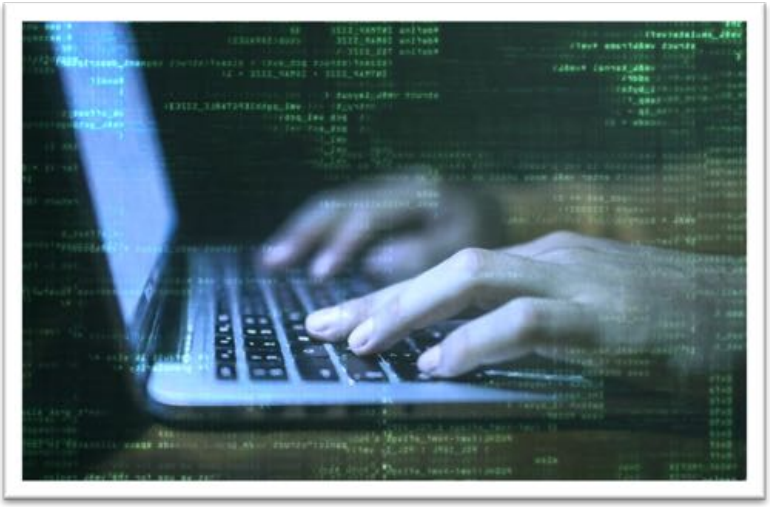
Keyword searches should be conducted on the merchant's website, including words such as "sedation," "bestiality," and "lolita." It may be helpful to determine whether the merchant has the ability to restrict sales by IP address for certain countries. Commercial CP companies have been known to block payments from the countries in which they are located and where they bank in order to avoid detection by local LE. It may be beneficial to retain a website's original source code for future review and comparison to the current website to identify changes in the products sold or new links to outside websites.[9] A monthly review of websites is recommended, and third-party vendors can be utilized for this purpose. Use of a third-party company that uses web crawling or spidering services to review entire merchant sites—computer programs designed to systematically browse the internet for specific content—is also beneficial.[7]

Institutions should also maintain awareness of countries that are at heightened risk for production or distribution of CP, as well as countries identified as high-risk sources of, or destinations for, child sex tourism, to the extent that this information is available. For example, IWF's report identifies the Netherlands as the highest risk country in terms of hosting abusive images online.[11]

Targeted Training for Financial Crimes Professionals

The TTPs associated with CP are evolving, and including ever more technical internet platforms. Thus, FIs should implement more targeted training programs that address investigative procedures and institution policy pertaining to CP and related crimes that are difficult to detect and subsequently report. As we've seen, child sexual exploitation increasingly involves cybercrime, with the majority of child sex trafficking currently occurring online, facilitated through internet ads. Consequently, it is necessary to be educated on new payment mechanisms, website types, the dark web, virtual worlds and currencies, and emerging TTPs utilized by abusers, consumers, and commercial CP providers. FIs should strengthen dialogue with other industries, including LE, and align SAR reporting with LE needs.

Suspicious Activity Reports (SAR)



Improvements to the SAR form itself are also vitally important, but due to the costly nature of SAR form updates, changes can take time.[2] As there is not currently a SAR predicate offense checkbox specific to CP, child sexual exploitation, or HT/HS, FIs should ensure that SAR narratives are as thorough, clear, and complete as possible. SAR filings, including all supporting documentation, should contain consistent file naming conventions. SAR filings should contain consistent predicate offense names and appropriate language and keywords so they can be optimally leveraged by LE.

Financial crimes professionals also have a responsibility to advocate for improved filing processes. Joann Alicea, CFCI, Senior Compliance Officer at JPMorgan Chase, has been a long-term advocate for an improved filing form.[2] In a 2011 ACAMS Today article, she advocated for an updated SAR form to include specific HT/HS predicate offense checkboxes and encouraged FinCEN to issue an alert calling for specific narrative text to facilitate better tracking by SAR

review teams.[1] In 2014 FinCEN released Guidance A008 calling for specific verbiage required in the SAR narrative, so that HT and HS reports could be accurately tracked. In February 2017 FinCEN released proposed revisions to the SAR form, which do include the addition of a checkbox for HT/HS. This is an excellent example of the way in which financial crimes professionals can recommend, advocate for, and effect change.

Conclusion

Crimes against children are a huge issue, but together we can be part of the solution. FIs should develop targeted training programs specific to child sex crimes and other predicate offenses; enhance suspicious activity reporting processes; advocate for and recommend SAR enhancements to FinCEN; and work collaboratively with front-line business units, LE, and other organizations that share the same purpose. CP and child sexual exploitation exist and thrive in a murky environment, and each industry sees only a piece of the puzzle. By working together, the pieces can align and provide valuable patterns of evidence that can be used to stop illegal activity, work toward prosecutions, and most importantly, rescue victims.

Is your financial institution at risk of being misused for illicit activity related to child pornography and child sexual exploitation? Our subject matter experts within the Financial Crimes Advisory practice at AML RightSource are highly skilled at helping institutions bolster their BSA program by developing and implementing a targeted and coordinated investigative approach to an array of criminal endeavors. Let us help you strengthen your policies and procedures so you can protect your institution against crimes that exploit children. Please visit http://amlrightsource.com/financial-crimes-advisory-services/ to find out more about the services we provide.

References

1. Alicea, Joann. "*$5.00 to Ruin the Life of Children and Women: Internet Ad Sites Used to Launder Money in Promoting Prostitution/Human Trafficking*." ACAMS Today, 2 Sept. 2011, http://www.acamstoday.org/internet-ad-sites-used-launder-money-promoting-prostitution/

2. Alicea, Joann. "*Joann Alicea: The Fight Against Human Trafficking/Smuggling Continues*." By Amy Wotapka. ACAMS Today, 9 Jun. 2017, http://www.acamstoday.org/joann-alicea-the-fight-against-human-traffickingsmuggling-continues/

3. "*Backpage.com's Knowing Facilitation of Online Sex Trafficking*." United States Senate, Permanent Subcommittee on Investigations, 20 Jan. 2017, https://www.mccaskill.senate.gov/imo/media/doc/2017.01.10%20Backpage%20Report.pdf

4. Collins, Wildred. *"IWF Report Shows Tech Behind Dark World of Online Child Abuse."* Alphr, 4 Apr. 2017, http://www.alphr.com/security/1005697/iwf-report-shows-tech-behind-dark-world-of-online-child-abuse

5. *"Commercial Child Pornography: A Brief Snapshot of the Financial Coalition Against Child Pornography."* National Center for Missing & Exploited Children, 2016, http://www.missingkids.com/content/dam/ncmec/en_us/documents/commercialchildpornographyabriefsnapshotofthefcacp2016.pdf

6. *"Extraterritorial Sexual Exploitation of Children."* The United States Department of Justice, 25 Jan. 2016, https://www.justice.gov/criminal-ceos/extraterritorial-sexual-exploitation-children

7. *"Financial Coalition Against Child Pornography Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography."* Financial Coalition Against Child Pornography, 1 Feb. 2011, http://www.missingkids.com/content/dam/ncmec/en_us/archive/documents/fcacptrendsinonlinecrimepaper2011.pdf

8. Hawke, Angela, and Raphael, Alison. *"The Global Study Report on Sexual Exploitation of Children in Travel and Tourism."* ECPAT International, May 2016, http://globalstudysectt.org/wp-content/uploads/2016/05/Global-Report-Offenders-on-the-Move-Final.pdf

9. *"Internet Merchant Acquisition and Monitoring Best Practices for the Prevention and Detection of Commercial Child Pornography."* Financial Coalition Against Child Pornography, May 2007, https://www.missingkids.org/content/dam/ncmec/en_us/internetmerchantacquisitionmay2007.pdf

10. *"Internet Merchant Acquisition and Monitoring Sound Practices to Help Reduce the Proliferation of Commercial Child Pornography."* Financial Coalition Against Child Pornography, Mar. 2016, https://www.missingkids.org/content/dam/ncmec/en_us/publications/fcacpsoundpractices.pdf

11. *"IWF Annual Report 2016."* Internet Watch Foundation, 3 Apr. 2017, https://annualreport.iwf.org.uk/

12. Parker, Luke. *"Backpage Goes Bitcoin-Only."* Brave New Coin, 9 Jul. 2015, https://bravenewcoin.com/news/backpage-goes-bitcoin-only/

13. *"The SAR Activity Review, Trends, Tips, & Issues, Issue 23."* Financial Crimes Enforcement Network BSA Advisory Group, May 2013, pp. 67-69, https://www.fincen.gov/sites/default/files/shared/sar_tti_23.pdf