Best Practices for Partnering with Law Enforcement

In This Report

Executive Summary[1]

01

The rapid digitization of consumers' lives, furthered by the increase in online spending due to COVID-19, has spawned profitable criminal enterprises that adversely impact businesses domestically and abroad. Cybercrime remains a lucrative enterprise that, according to crime reports filed with the Federal Bureau Investigation's (FBI's) Internet Crime Complaint Center in 2019, causes losses exceeding $3.5 billion annually.[2] In 2018, the White House Council of Economic Advisors estimated that malicious cyber activity cost the U.S. economy from $57 billion to $109 billion in 2016 alone.[3] The proliferation of digital and human targets contributes to these statistics, providing an attack surface that shows no signs of shrinking.

The number of businesses falling victim to cybercrime in the digital advertising industry has also increased. The impact of digital ad crime on companies is significant, causing large-scale financial damage, reputational harm, and legal jeopardy. As criminals exploit the evolving digital advertising landscape to engineer new attacks, industry, working with law enforcement, should collaborate more effectively to stop them. By creating a culture that encourages proactive industry efforts to prevent fraud, early sharing of threat intelligence, and reporting of crimes to law enforcement, the digital ad industry can thwart cyber criminals and aid in their apprehension, thereby preventing or deterring them from committing future crimes that victimize the digital advertising supply chain and innocent consumers.

Digital advertising organizations can take a critical step toward protecting themselves and dismantling criminal infrastructure by partnering with law enforcement. Law enforcement agencies are uniquely positioned to preempt and respond to crime at scale, as they possess tools, legal authorities, and international law enforcement relationships that are unavailable to private entities. These resources can greatly increase the odds of successfully apprehending attackers and discouraging would-be perpetrators from engaging in illicit activity across the digital ad supply chain.

The bottom line is that digital advertising industry companies are targeted by cyber criminals and thus can be victims of cybercrime. Law enforcement is here to help them, and to prevent others from being victimized. The scope of criminal activity affecting the digital advertising industry and its effect on the supply chain are immense. Ad fraud, malvertising, and piracy are lucrative crimes, and companies should work together and with law enforcement to disrupt these criminal operations and the stream of illicit profit they generate. By adopting "best practices" for working with law enforcement, the digital advertising industry can ensure that this partnership is successful. Public and private sector collaboration is a critical ingredient to building consumer trust in the industry, systemically toppling criminal enterprises, and bringing criminals to justice.

---

[1] This white paper is intended to help organizations prepare for and respond to cyber incidents. It does not, however, confer any rights or remedies and does not have the force of law. See United States v. Caceres, 440 U.S. 741 (1979). Furthermore, the Criminal Division of the U.S. Department of Justice is proud to partner with TAG in producing this white paper in support of our work combating crime on online platforms; however, this paper should not be interpreted to be an endorsement of TAG products or services.

[2] "2019 Internet Crime Report," Federal Bureau of Investigation Internet Crime Complaint Center, 2019.

[3] "The Cost of Malicious Cyber Activity to the U.S. Economy," U.S. White House, The Council of Economic Advisers, February 2018.

02.

Solving Billion Dollar Problems:

Fraud, Piracy, and Malvertising

Fraud, piracy, and malvertising degrade consumer trust in the digital advertising industry and stymie industry growth by diverting ad revenue to criminals. Cyber criminals rely on the complexity of the digital advertising supply chain to defraud the community and consumers, using a variety of profit-generating methods to adapt to the ever-changing landscape. This fraud fosters a scaled criminal economy that results in billions of dollars in digital advertising losses annually.

Ad fraud is malicious traffic in the digital advertising supply chain that is used by criminals to steal significant sums of revenue. Ad fraud encompasses a variety of criminal techniques such as botnets, clickjacking, hidden ads, and fake installation. These methods fraudulently represent online advertisement impressions, clicks, or conversions to consumers to generate significant financial gain. Although anti-fraud programs are having a demonstrable impact, evolving criminal techniques make ad fraud an ongoing threat across a range of existing and emerging media.

Digital piracy is the illegal practice of digitally copying, distributing, viewing, and using copyright-protected content, such as videos, music, and software, without authorization. Digital piracy causes significant financial losses. Ads placed on digital pirates' sites also pose significant reputational concerns for advertisers. The 2015 study also concluded that infringed content represents the most significant portion of lost revenue opportunity costs, driven by the ease of use and direct access to unlawfully obtained free content by consumers.

While the term malware can mean malicious software of any sort delivered by any means, “malvertising” refers to the use of digital advertisements – including creative tags and landing pages – specifically to distribute malware, often for financial gain. Malvertising plagues the digital ad ecosystem and creates costs for participants.

There are also intangible costs associated with malvertising, and loss of consumer trust is at the top of that list.

The scope of criminal activity in the digital advertising industry and its repercussions on the supply chain are immense. Ad fraud, digital piracy, and malvertising are lucrative crimes that cause significant economic and reputational harm. Companies must work together and with law enforcement to disrupt these criminal operations and their streams of illicit profit. By partnering to fight criminal activity across the supply chain, the digital advertising industry can help to build trust among consumers and content creators and to bring criminals to justice.

03

Why Involve Law Enforcement?

Apprehending cyber criminals and disrupting their operations impose costs on cyber criminals to deter them from continuing to attack the digital ad supply chain. By partnering with law enforcement to track incidents, thwart attacks, and pursue prosecution, the digital advertising community can discourage criminals from committing crimes and dismantle the infrastructure they use to stage attacks. By adopting a proactive approach, the digital advertising industry can enable law enforcement to play a critical role in preempting and preventing criminal activity, and not just responding to it.

The principal federal law enforcement agencies responsible for investigating malicious cyber activities like botnets and malware are the FBI and U.S. Secret Service (Secret Service). These efforts are supplemented by the National Intellectual Property Rights Coordination Center (IPR Center), which works at the forefront of the U.S. government's response to global intellectual property (IP) theft and enforcement of U.S. international trade laws. The Department of Justice's Computer Crime and Intellectual Property Section, working with the 94 U.S. Attorney's Offices nationwide, specializes in prosecuting cybercrimes and intellectual property crimes.

Law enforcement agencies are in a unique position to deter cybercrimes like ad fraud, malvertising, and digital piracy on a large scale. They can disrupt and stop ongoing criminal activity through arrest and prosecution and generally deter others from engaging in similar activity. Law enforcement agencies understand the tactics, techniques, and procedures used by threat actors. Furthermore, they have access to intelligence and resources that allow them considerable insight into specific crimes. For instance, an investigation of one criminal organization can yield valuable information about the tradecraft used by similar criminal enterprises. Law enforcement agencies also rely on unique domestic and international resources and relationships to fight transnational criminal organizations. For example, federal law enforcement can quickly preserve digital evidence in more than 80 countries through collaboration with

international law enforcement partners. Law enforcement agencies can also deter foreign criminals by having them extradited to the United States for prosecution, assisting in foreign prosecutions, or supporting the imposition of economic or diplomatic responses, such as sanctions or blacklisting.[4] Law enforcement's international reach is especially important to battling crime involving digital advertising, as ad fraud rings often operate without regard to jurisdictional boundaries.

Law enforcement investigations of cybercrimes committed against the digital advertising industry begin with the premise that the affected companies and their customers are victims, and law enforcement is here to help them. But law enforcement cannot act unless it learns that a crime has been committed, and victims of crime are typically in the best position to detect and report malicious activity. This underscores the need for the digital advertising industry to develop a culture of engaging and appropriately sharing information with law enforcement. Effective prosecution of intellectual property crime requires significant assistance from its victims.[5] Once these crimes are reported, federal law enforcement authorities need to quickly investigate and preserve ephemeral digital evidence. Early referral to law enforcement is the best way to ensure that evidence of a crime is properly secured and that all investigative avenues are available to bring perpetrators to justice.

Organized cybercrime requires a coordinated response from law enforcement and the private sector. Leveraging the digital advertising industry's collective knowledge to help law enforcement conduct investigations that result in appropriate criminal sanctions can be a significant deterrent to the crimes plaguing the industry today. By partnering with law enforcement to detect and respond to activity in the digital ad supply chain, we can hold cyber criminals accountable, prevent future incidents, and disrupt the infrastructure they use to stage damaging attacks against consumers and the digital advertising industry.

---

[4] "Reporting Intellectual Property Crime: A Guide for Victims of Copyright Infringement, Trademark Counterfeiting, and Trade Secret Theft," U.S. Department of Justice, October 2018.
[5] Id.

The Importance of Threat Intellegence Sharing

Intelligence sharing is a critical component of combating cyber threats. Awareness of the evolving nature of fraud and malvertising is key to staying ahead of emerging threats and achieving greater success in preventing attacks and remediating any resulting damage. Building a successful threat intelligence sharing culture within the digital advertising industry offers tremendous benefits to both individual organizations and the industry at large. Simply put, sharing threat intelligence on a consistent basis helps organizations better protect their assets across the digital advertising supply chain.

Threat intelligence sharing through mechanisms like Information Sharing and Analysis Organizations (ISAOs) provides critical context on the wide swath of malicious activity targeting the digital advertising industry and fosters a more accurate understanding of potential threat vectors, attack methods, and threat actor techniques. Organizations that participate in regular threat sharing receive a holistic view of industry-wide threats, positioning them to close the gap between detection and defensive measures and enrich their own investigations. Expedient intelligence sharing can also prevent a single threat from creating a cascade of damage across the digital ad ecosystem, preying upon industry practices shared in common without the corresponding information sharing. Sharing arrangements also provide access to a network of industry-specific threat knowledge and expertise, which can be especially useful in an interconnected ecosystem like digital advertising that relies on complex transaction chains to publish digital ads.

Sharing enables the digital advertising industry to enhance its cyber defense capabilities by leveraging the knowledge and experience of the broader community. By correlating and sharing actionable threat intelligence on a regular basis, participants from across the digital ad supply chain can work to improve the collective security posture of the entire industry and defeat future threats. The digital ad industry has the opportunity to meaningfully deter criminals by creating a culture that encourages routine sharing of intelligence about threats and cyber incidents with one another and law enforcement.

04

Liability and Legal Protections for Threat Intelligence Sharing

The sharing of cyber threat information within ISAOs such as TAG is protected from liability when shared in accordance with the Cybersecurity Information Sharing Act of 2015 (CISA 2015). In October 2020, the Department of Homeland Security (DHS) and DOJ published a revision of the Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defense Measures with Federal Entities under the Cybersecurity Information Sharing Act (CISA) of 2015, which explains in detail how to share and receive information (specifically "cyber threat indicators" and "defensive measures") under CISA 2015. The liability protection under CISA 2015 also extends to communications between non-federal and federal entities about cyber threat indicators and defensive measures that meet CISA 2015's requirements.[6]

Consistent with CISA 2015, Information Sharing and Analysis Centers (ISACs) and ISAOs are also encouraged to further disseminate to their membership cyber threat information and threat intelligence received from federal entities that qualify as cyber threat indicators or defensive measures.[7] When that information is shared in accordance with CISA 2015, it receives liability protection for the act of sharing. Private organizations sharing information with ISAOs and ISACs in accordance with CISA similarly receive liability protection. ISACs, ISAOs, and other private organizations also are encouraged to share such information with federal entities, consistent with CISA 2015 and subject to any legal obligations and are eligible for CISA 2015's liability protection for doing so.

> "Law enforcement treats information collected during a criminal investigation as sensitive information that is safeguarded from unwarranted or unnecessary disclosure."

Aside from liability protection, organizations that report incidents or other information to law enforcement receive certain additional legal protections. Law enforcement treats information collected during a criminal investigation as sensitive information that is safeguarded from unwarranted or unnecessary disclosure. In addition, the Freedom of Information Act (FOIA) exempts certain records or information gathered for law enforcement purposes from disclosure. CISA 2015 also affords protection from state and federal disclosure laws when cyber threat indicators are shared with the FBI, Secret Service, or another federal entity consistent with CISA 2015.[8] In addition, the FTC and SEC have affirmed that they view companies that report data breaches and cyber incidents to law enforcement and cooperate with the subsequent investigation more favorably than those who do not. Though law enforcement does not routinely disclose evidence that it gathers during its cyber investigations to regulators, DOJ is willing to inform regulatory agencies of any cooperation that a company facing a regulatory inquiry has furnished to it, when the company requests that DOJ do so.

[6] CISA's liability protections can also extend to communications with law enforcement agencies about cyber threat indicators and defensive measures that were previously shared with DHS pursuant to CISA 2015. "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015," The Department of Homeland Security and the Department of Justice, October 2020.

[7] CISA 2015 defines cyber threat indicators and defensive measures. See 6 U.S.C. §§ 1501(6) and (7).

8 See 6 U.S.C. §§1503(c) and (d)(4)(B), 1504(d)(3). See also "Best Practices for Victim Response and Reporting of Cyber Incidents," DOJ Computer Crime & Intellectual Property Section, September 2018.

05

Best Practices for Partnering with Law Enforcement

By partnering with law enforcement, organizations within the digital advertising supply chain can play a significant role in helping law enforcement investigate criminals, dismantling the digital infrastructure used by criminals, and protecting the digital ad supply chain. Law enforcement agencies well-versed in tracking and apprehending criminals have provided best practices for private sector organizations to work with them regarding threat sharing and responding to criminal activity.[9] Everyone in the digital advertising industry can benefit from following simple and proven effective best practices identified in that guidance, a number of which are highlighted below.

[9] For example: "Best Practices for Victim Response and Reporting of Cyber Incidents," DOJ Computer Crime & Intellectual Property Section, September 2018, and "Preparing for a Cyber Incident," U.S. Secret Service Cybercrime Investigations.

Get Your House In Order

Preparedness is critical when responding to—and preventing—cyber incidents. Organizational preparedness within the digital advertising industry will aid you and law enforcement in addressing criminal activity more expediently and will help limit detrimental impacts to victims.

- **Educate senior management about threats to digital advertising.** Help create a common understanding of the impact digital advertising threats have on your organization's bottom line and reputation. Establish routine briefings and outline risk scenarios that address the scope and severity of threats.

- **Have an actionable plan in place.** Organizations should have concrete procedures to follow in the event that they are victims of digital advertising crimes and ensure that internal policies and rules are in place to familiarize personnel with these procedures in advance. Having an actionable plan also assists law enforcement in understanding the steps already taken during an incident so law enforcement can better prepare an investigation or response.

- **Make sure your basic cybersecurity procedures are up-to-date.** Commonsense cybersecurity practices are at the foundation of effective cybercrime deterrence. Keep up-to-date on the latest recommendations on best practices from government and private sector sources. In particular, ensure that your organization's program includes reasonable patch and password management programs, multi-factor authentication, and an appropriate perimeter defense, such as a firewall. You will also want to enable logging on your servers and maintain copies of logs for as long as practicable, as these logs will be critical for any internal or criminal investigations of cyber incidents.

- **Procure appropriate cybersecurity technology and services before an incident occurs.** Organizations should have ready access to the technology and services they will need to respond to and recover from cyber incidents. Make sure that your intrusion detection or prevention, anti-malware, and anti-fraud vendors are accounted for in preparedness planning. You may also want to consider identifying or retaining an incident response firm to expedite your response to a cyber incident. In considering such a firm, you will want to ensure that it has experience with applicable laws and regulations, is using forensically sound methods that will preserve potential evidence and data, and has well established channels of communication with law enforcement.

- **Ensure your legal counsel is familiar with technology and cyber incident management.** Decisions made during an incident may have legal consequences down the road. Having ready access to legal counsel who are well-versed in cybercrime and cyber incidents, as well as the relevant technology, can speed up an organization's decision making and ensure response activities are legally sound.

See The Big Picture

Organizations are more likely to have intelligence at a scale that law enforcement can act upon when you combine forces with others within–and outside–the digital advertising industry to piece together the bigger picture.

Establish relationships with private and public cyber Information-Sharing and Analysis Organizations (ISAO). Proactive information sharing helps build industry resilience against evolving threats. Get involved in ISAO programs to share information about threats you see and stay abreast of new and emerging threats that could affect your campaigns. Encourage your partners to do the same so that they can better protect your assets across the digital advertising supply chain.

Make connections with law enforcement. Identify key contacts responsible for cybercrime at local FBI and Secret Service field offices and maintain regular contact to cultivate good working relationships that could prove invaluable when you need law enforcement assistance. This will also help establish a relationship that will foster two-way communications and information-sharing that will be beneficial to both your organization and law enforcement.

FBI Cyber Crime Unit

U.S. Secret Service

Internet Crime Complaint Center ("IC3")

Bolster your intelligence collection sources. In addition to information sharing to and from ISAOs and peers within the digital advertising industry, law enforcement is also a valuable source of cyber threat intelligence. The FBI and Secret Service regularly share cyber threat data with the private sector through established programs. DHS's Cybersecurity & Infrastructure Security Agency (CISA) is also a valuable source of cyber threat and mitigation information.[10] The data that these federal entities provide contains alerts and analysis that can help organizations detect, prevent, and mitigate attacks.

[10] For a link to some of the resources available through CISA, see https://us-cert.cisa.gov/resources, and for information on its national cyber awareness system, see https://us-cert.cisa.gov/ncas.

Act Fast

When you are concerned about a possible cyber attack, it is important to quickly gather the information that you need to stop the cyber attack and that law enforcement will need to prosecute the criminals behind the attack.

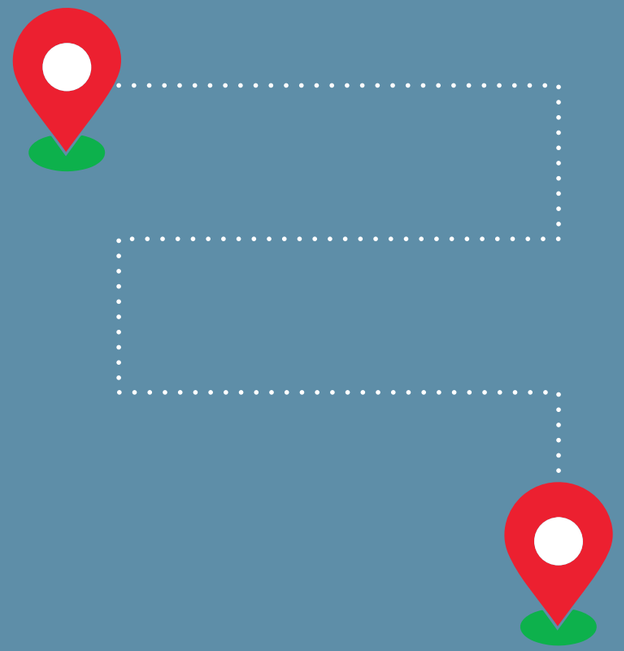
- **Engage with law enforcement before an incident.** When you notice malicious events, it is imperative to act quickly. Often what may seem like a one-off incident is connected to large-scale criminal activity. Law enforcement can assist in connecting the dots and tracking down the criminals responsible. Routine threat sharing with law enforcement is one important way to stay on top of threats.

- **Contact law enforcement right away.** In the event of an incident, early referral is the best way to ensure that law enforcement acts quickly. In some cases, early action can help law enforcement stop the threat before an attack takes place.

- **Stop using compromised systems**. If you believe your system is compromised, avoid using it, to the extent reasonably possible. In particular, do not use a system suspected of being compromised to communicate about mitigation strategies or responses.

- **Document all investigative steps.** To avoid duplication of effort and retracing of steps, internal investigations and other response activities should create a record of all investigative steps that can later be presented to law enforcement.

- **Preserve the evidence.** Evidence is critical to apprehending cyber criminals, disrupting ongoing schemes, and taking down criminal infrastructure. Any physical, documentary, or digital evidence acquired during an internal investigation should be preserved for later use in legal proceedings. Make sure evidence and data is preserved with forensically sound methods that do not taint or destroy the evidence so it may be used in prosecutions and court proceedings initiated to take down criminal infrastructure and hold perpetrators accountable.



Stay The Course

Successful prosecution of digital crimes depends on cooperation between victims and law enforcement. It is imperative that organizations be patient during an investigation and expect that success will take time.

Share the results of internal investigations and lawsuits. As with any suspected crime, victims may provide law enforcement with information gathered from internal investigations of intellectual property theft or other cyber incidents. In addition, unless a court has ordered otherwise, victims may generally provide law enforcement with any evidence or materials developed in civil suits, such as intellectual property enforcement actions. These include court pleadings, deposition testimony, documents, and written discovery responses.

Remain vigilant. Even after a cyber incident appears to be under control, organizations should remain alert. It is common for criminals to attempt attacks a second or third time, especially when they have an increased understanding of the landscape. Sophisticated criminals have become adept at maintaining a hidden presence on systems they have compromised. Victim organizations should continue watching for anomalous activity and alert law enforcement in the event anomalous activity is detected.

Conclusion

> "
>
> **The digital ad industry has the potential to combat cybercrime by creating a culture that fosters and promotes routine community-wide threat sharing and reporting crimes to law enforcement.**
>
> "

Stopping organized cybercrime from targeting the digital advertising industry requires a coordinated response. Leveraging the industry's collective knowledge to impose consequences on those committingcriminal acts will deter the criminals who are plaguing the industry today. The digital ad industry has the potential to combat cybercrime by creating a culture that fosters and promotes routine community-wide threat sharing and reporting crimes to law enforcement. Law enforcement agencies are uniquely positioned to fight criminal activity because of the investigative tools, insights, and resources available to them. By partnering with law enforcement to detect and respond to activity in the digital ad supply chain, we will also disrupt the infrastructure used by criminals, thwart the commission of even more significant attacks, and prevent and deter future cyber incidents.

The scope of criminal activity in the digital advertising industry and its repercussions on the supply chain are immense. The bottom line is that ad fraud, digital piracy, and malvertising are lucrative crimes, and companies must work together and with law enforcement to disrupt the criminal operations that commit them and interrupt the stream of illicit revenue they produce. By partnering to fight criminal activity across the supply chain, the digital advertising industry is helping to build trust among consumers and content creators and helping to bring criminals to justice.

06

tagtoday.net