Reporting Intellectual Property Crime:

A Guide for Victims of Counterfeiting, Copyright Infringement, and Theft of Trade Secrets

The United States Department of Justice's Task Force on Intellectual Property Enforcement

Reporting Intellectual Property Crime: A Guide for Victims of Counterfeiting, Copyright Infringement, and Theft of Trade Secrets

Contents

What are Copyrights, Trademarks and Trade Secrets?

The United States has created enforceable rights in "intangibles" that are known as intellectual property, including copyrights, trademarks and trade secrets. ***Copyright law*** provides federal protection against infringement of certain exclusive rights, such as reproduction and distribution, of "original works of authorship," including computer software, literary works, musical works, and motion pictures. The use of a commercial brand to identify a product is protected by ***trademark law***, which prohibits the unauthorized use of "any word, name, symbol, or device" used by a person "to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods." Finally, trade secret law provides legal protection for any formula, device, or compilation of information used in a business from being disclosed without the owner's permission. However, legal protection is only afforded to those trade secrets that possess independent economic value and which the owner has taken reasonable measures to keep secret.

How Can Intellectual Property Be Stolen?

Intellectual property may be stolen or misappropriated in many ways. A copyrighted work may be illegally infringed by making and selling an unauthorized copy, as with infringing computer software. A trademark may be infringed by selling a good with a counterfeit mark. A trade secret may be stolen from its owner and used to benefit a competitor.

What Types of Intellectual Property Theft Constitute a Federal Crime?

Although civil remedies may provide compensation to wronged intellectual property rights holders, criminal sanctions are often warranted to ensure sufficient punishment and deterrence of wrongful activity. Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation and ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business for defendants. Among the most significant provisions are the following:

Counterfeit Trademarks: The Trademark Counterfeiting Act, 18 U.S.C. § 2320(a), provides penalties of up to ten years imprisonment and a $2 million fine for a defendant who "intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services."

Counterfeit Labeling: The counterfeit labeling provisions of 18 U.S.C. § 2318 prohibit trafficking in counterfeit labels designed to be affixed to phono records, copies of computer programs, motion pictures and audiovisual works, as well as trafficking in counterfeit documentation or packaging for computer programs. Violations are punishable by up to 5 years imprisonment and a $250,000 fine.

Criminal Copyright Infringement: Copyright infringement is a felony punishable by up to 3 years imprisonment and a $250,000 fine under 17 U.S.C. § 506(a) and 18 U.S.C. § 2319 where a defendant willfully reproduces or distributes at least 10 copies of one or more copyrighted works with a total retail value of more than $2,500 within a 180_day period. The maximum penalty rises to 5 years imprisonment if defendant acted "for purposes of commercial advantage or private financial gain." Misdemeanor copyright infringement occurs where the value exceeds $1,000.

Theft of Trade Secrets: The Economic Espionage Act contains two separate provisions that criminalize the theft of trade secrets. The first provision, 18 U.S.C. § 1831(a), prohibits thefts of the trade secrets for the benefit of a foreign government or agent, and is punishable by up to 15 years imprisonment and a $500,000 fine. The second, 18 U.S.C. § 1832, prohibits thefts of commercial trade secrets, and is punishable by up to 10 years imprisonment and a $250,000 fine. The statute broadly defines the term "trade secret" to include all types of information which the owner has taken reasonable measures to keep secret and which has independent economic value.

Confidentiality: Federal law also provides special protections to victims in trade secret cases to preserve the confidentiality of the information during criminal proceedings. The statute provides that courts "shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C. § 1835.

Why Should You Report Intellectual Property Crime?

Intellectual property is an increasingly important part of the United States' economy, representing its fastest growing sector. For example, in 2002 copyright industries alone contributed approximately 6%, or $626 billion, to America's gross domestic product, and employed 4% of America's workforce, according to an economic study commissioned by the International Intellectual Property Alliance. As the nation continues to shift from an industrial economy to an information-based economy, the assets of the country are increasingly based in intellectual property.

In recognition of this trend, the Department of Justice is waging the most aggressive campaign against the theft and counterfeiting of intellectual property in its history. The priority of criminal intellectual property investigations and prosecutions nationwide has been increased, and additional resources on both the prosecutive and investigative levels have been brought to bear on the growing problem of intellectual property theft.

Effective prosecution of intellectual property crime, however, also requires substantial assistance from its victims. Because the holders of intellectual property rights are often in the

best position to detect a theft, law enforcement authorities cannot act in many cases unless the crimes are reported in the first place. Once these crimes are reported, federal law enforcement authorities need to quickly identify the facts that establish jurisdiction for the potential intellectual property offenses, such as federal copyright and trademark registration information, as well as facts concerning the extent of victim's potential loss, the nature of the theft and possible suspects. In a digital world where evidence can disappear at the click of a mouse, swift investigation is often essential to successful intellectual property prosecutions.

Accordingly, the Department of Justice has created this handbook to facilitate the flow of critical information from victims of intellectual property crimes to law enforcement authorities. The Department of Justice's aim is to make it as easy as possible to report incidents of intellectual property crime to law enforcement authorities, including whom to call and what to tell them.

Note: The guidelines set forth below seek information that, in the experience of Department of Justice prosecutors and investigators, is useful or even critical to the successful prosecution of the most common intellectual property crimes. These guidelines are not intended to be exhaustive, nor does the presence or absence of responsive information from the victim necessarily determine the outcome of an investigation.

What Should You Do if You are Victimized?

Victims of intellectual property crime such as counterfeiting and theft of trade secrets often conduct internal investigations before referring matters to law enforcement. These investigations can encompass a variety of investigative steps, including interviews of witnesses, acquisition of counterfeit goods, surveillance of suspects, and examination of computers and other evidence. Victims can maximize the benefit of these independent investigative activities as follows:

1. Document All Investigative Steps: To avoid duplication of effort and retracing of steps, internal investigations should seek to create a record of all investigative steps that can later be presented to law enforcement, if necessary. If a victim company observes counterfeit goods for sale online and makes a purchase, for example, investigators should record the name of the Web site, the date and time of the purchase, the method of payment, and the date and manner of delivery of the goods. Any subsequent examination of the goods should then be recorded in a document that identifies the telltale characteristics of theft or counterfeiting, such as lack of a security seal, poor quality or the like.

Similarly, in the case of a suspected theft of trade secrets, any internal investigation or surveillance of the suspect, or a competitor believed to be using the stolen information, should be recorded in writing. A record of any interviews with suspects or witnesses should be made by tape or in writing. The pertinent confidentiality agreements, security policies and access logs should also be gathered and maintained to facilitate review and reduce the risk of deletion or destruction.

2. Preserve the Evidence: Any physical, documentary or digital evidence acquired in the course of an internal investigation should be preserved for later use in a legal proceeding. In the online theft example identified above, victims should print-out or obtain a digital copy of the offending Web site and safely store any infringing goods and their packaging, which may contain valuable details of their origin. If the computer of an employee suspected of stealing trade secrets has been seized, any forensic analysis should be performed on a copy of the data, or "digital image," to undermine claims that the evidence has been altered or corrupted.

3. Contact Law Enforcement Right Away: Victims can maximize their legal remedies for intellectual property crime by making contact with law enforcement soon after its detection. Early referral is the best way to ensure that evidence of an intellectual property crime is properly secured and that all investigative avenues are fully explored, such as the execution of search warrants and possible undercover law enforcement activities. Communication with law enforcement authorities at the onset of suspected violations also allows a victim to coordinate civil proceedings with possible criminal enforcement. Use the reporting guides set forth later in this document to organize the information you gather and provide the necessary information to your law enforcement contact.

How Can You Assist Law Enforcement?

Prosecutions of intellectual property crime often depend on cooperation between victims and law enforcement. Indeed, without information sharing from intellectual property rights holders, prosecutors can neither discern the trends that suggest the most effective overall enforcement strategies, nor meet the burden of proving the theft of intellectual property in a specific case. The following seeks to provide guidance concerning the types of assistance that may be offered by victims of intellectual property theft to law enforcement authorities.

Identify Stolen Intellectual Property: Just as in cases involving traditional theft, such as a burglary or shoplifting, victims of intellectual property theft may – and often must – assist law enforcement in the identification of stolen property. Thus, law enforcement may call upon a victim representative or expert to examine items obtained during an investigation to determine their origin or authenticity. In a copyright infringement or trademark investigation, for example, an author or software company may be called upon to analyze CDs or other media that appear to be counterfeit, while a victim representative in a theft of trade secret case may be asked to review documents or computer source code. Prosecutors may later the seek expert testimony from the victims at trial.

In certain investigations, law enforcement agents also may request a victim's presence during the execution of a search warrant to help the agents identify specific items to be seized. In those circumstances, the victim's activities will be strictly limited to those directed by supervising law enforcement agents.

Share the Results of Internal Investigations or Civil Lawsuits: As with any suspected crime, victims may provide law enforcement with information gathered as a result of internal investigations into instances of intellectual property theft. This handbook contains a section on "Gathering Information on Suspected Intellectual Property Crime" to provide guidance on how a victim can maximize the benefit of any internal investigations it chooses to conduct. In addition, unless the proceedings or information has been ordered sealed by a court, victims may generally provide law enforcement with any evidence or materials developed in civil intellectual property enforcement actions, including court pleadings, deposition testimony, documents and written discovery responses.

Participate in Law Enforcement Task Forces: Federal, state and local law enforcement agencies and prosecutors all over the country have formed task forces to combat computer and intellectual property crime and to promote information sharing between government and industry. The United States Secret Service, for example, has created Electronic Crimes Task Forces in 13 cities, and the Federal Bureau of Investigation has founded more than 60 "Infragard" chapters around the country. In addition, many areas have "high-tech crime" task forces that investigate intellectual property theft. Members of the intellectual property industry are encouraged to participate in these organizations to establish law enforcement contacts that will enable these members to quickly respond to incidents of intellectual property and other crime. (Information on joining these organizations is available on the Web at *www.ectaskforce.org* and *www.infragard.net*).

Contributions of Funds, Property, or Services: Donating funds, property, or services to federal law enforcement authorities can raise potential legal and ethical issues that must be addressed on a case-by-case basis. In general, federal law places limitations on contributions to law enforcement authorities.

Checklist for Reporting a Copyright Infringement or Counterfeit Trademark Offense

If you or your company have become the victim of a copyright infringement or counterfeit trademark offense, please fill out the information as indicated below and contact a federal law enforcement official to report the offense. An insert with contact information for law enforcement officials in your area should be included at the end of this guide.

Background and Contact Information:

1. Victim's Name:

2. Primary Address:

3. Nature of Business:

4. Contact:

Phone: Fax:

Email: Pager/Mobile:

Description of the Intellectual Property

5. Describe the copyrighted material or trademark (e.g., title of copyrighted work, identity of logo):

6. Is the copyrighted work or trademark registered with the U.S. Copyright Office or the Federal Patent and Trademark Office? ___ YES ___NO

   a. If so, please provide the following:

      i. Registration Date:

      ii. Registration Number:

      iii. Do you have a copy of the certificate of registration?

      iv. Has the work or mark been the subject of a previous civil or criminal enforcement action? If so, please provide a general description.

b. If not, state if and when you intend to register:

7. What is the approximate retail value of the copyrighted work or trademarked good?

Description of the Intellectual Property Crime

8. Describe how the theft or counterfeiting was discovered:

9. Do you have any examination reports of the infringing or counterfeit goods? ___YES ___NO.
(If so, please provide those reports to the law enforcement official).

10. Describe the scope of the theft or counterfeiting operation, including the following information:

a. Estimated quantity of illegal distribution:

b. Estimated time period of illegal distribution:

c. Is the illegal distribution national or international? Which states or countries?

11. Identify where the theft or counterfeiting occurred, and describe the location:

12. Identify the name(s) or location(s) of possible suspects, including the following information:

Name (Suspect #1):

Phone number:

Email address:

Physical address:

Current employer, if known:

Reason for suspicion:

Name (Suspect #2):

Phone number:

Email address:

Physical address:

Current employer, if known:

Reason for suspicion:

13. If the distribution of infringing or counterfeit goods involves the Internet (e.g., World Wide Web, FTP, email, chat rooms), identify the following:

    a. The type of Internet theft:

    b. Internet address, including linking sites (domain name, URL, IP address, email):

    c. Login or password for site:

    d. Operators of site, if known:

14. If you have conducted an internal investigation into the theft or counterfeiting activities, please describe any evidence acquired:

Civil Enforcement Proceedings

15. Has a civil enforcement action been filed against the suspects identified above? ___YES ___NO

    a. If so, identify the following:

        i. Name of court and case number:

        ii.Date of filing:

        iii. Names of attorneys:

        iv. Status of case:

    b. If not, is a civil action contemplated? What type and when?

16. Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Checklist for Reporting a Theft of Trade Secrets Offense

If you or your company have become the victim of a theft of trade secrets offense, please fill out the information indicated below and contact a federal law enforcement official to report the offense. An insert with contact information for law enforcement officials in your area should be included at the end of this guide.

NOTE ON CONFIDENTIALITY: Federal law provides that courts "shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C. § 1835. Prosecutors utilizing any of the information set forth below will generally request the court to enter an order to preserve the status of the information as a trade secret and prevent its unnecessary and harmful disclosure.

Background and Contact Information

1. Victim's Name:

2. Primary Location and Address:

3. Nature of Primary Business:

4. Law Enforcement Contact:

Phone: Fax:

Email: Pager/Mobile:

Description of the Trade Secret

5. Generally describe the trade secret (e.g., source code, formula):

Provide an estimated value of the trade secret identifying ONE of the methods and indicating ONE of the ranges listed below:

Method

___Cost to Develop the Trade Secret;

___Acquisition Cost (identify date and source of acquisition); or

___Fair Market Value if sold.

Estimated Value:

___Under $50,000;

___Between $50,000 and $100,000;

___Between $100,000 and $1 million;

___Between $1 million and $5 million; or

___Over $5 million

Identify a person knowledgeable about valuation, including that person's contact information:

General Physical Measures Taken to Protect the Trade Secret

6. Describe the general physical security precautions taken by the company, such as fencing the perimeter of the premises, visitor control systems, using alarming or self-locking doors or hiring security personnel.

7. Has the company established physical barriers to prevent unauthorized viewing or access to the trade secret, such as "Authorized Personnel Only" signs at access points? (See below if computer stored trade secret.) ___YES ___NO

8. Does the company require sign in/out procedures for access to and return of trade secret materials? ___YES ___NO

9. Are employees required to wear identification badges? ___YES ___ NO

10. Does the company have a written security policy? ___YES ___NO

    a. How are employees advised of the security policy?

    b. Are employees required to sign a written acknowledgment of the security policy? ___YES ___NO

    c. Identify the person most knowledgeable about matters relating to the security policy, including title and contact information.

11. How many employees have access to the trade secret?

12. Was access to the trade secret limited to a “need to know” basis? ___YES ___NO

Confidentiality and Non-Disclosure Agreements

13. Does the company enter into confidentiality and non-disclosure agreements with employees and third-parties concerning the trade secret? ___YES ___NO

14. Has the company established and distributed written confidentiality policies to all employees? ___YES ___NO

15. Does the company have a policy for advising company employees regarding the company’s trade secrets? ___YES ___NO

Computer-Stored Trade Secrets

16. If the trade secret is computer source code or other computer-stored information, how is access regulated (e.g., are employees given unique user names and passwords)?

17. If the company stores the trade secret on a computer network, is the network protected by a firewall? ___YES ___NO

18. Is remote access permitted into the computer network? ___YES ___NO

19. Is the trade secret maintained on a separate computer server? ___YES ____NO

20. Does the company prohibit employees from bringing outside computer programs or storage media to the premises? ___YES ___NO

21. Does the company maintain electronic access records such as computer logs? ___YES ___NO

Document Control

22. If the trade secret consisted of documents, were they clearly marked "CONFIDENTIAL" or "PROPRIETARY"? ___YES ___NO

23. Describe the document control procedures employed by the company, such as limiting access and sign in/out policies.

24. Was there a written policy concerning document control procedures, and if so, how were employees advised of it? ___YES ___NO

25. Identify the person most knowledgeable about the document control procedures, including title and contact information.

Employee Controls

26. Are new employees subject to a background investigation? ___YES ___NO

27. Does the company hold "exit interviews" to remind departing employees of their obligation not to disclose trade secrets? ___YES ___NO

Description of the Theft of Trade Secret

28. Identify the name(s) or location(s) of possible suspects, including the following information:

    Name (Suspect #1):

    Phone number:

Email address:

Physical address:

Employer:

Reason for suspicion:

Name (Suspect #2):

Phone number:

Email address:

Physical address:

Employer:

Reason for suspicion:

29. Was the trade secret stolen to benefit a third party, such as a competitor or another business? ___YES ___NO

If so, identify that business and its location:

30. Do you have any information that the theft of trade secrets were committed to benefit a foreign government or instrumentality of a foreign government? ___YES ___NO

If so, identify the foreign government and describe that information.

31. If the suspect is a current or former employee, describe all confidentiality and non-disclosure agreements in effect.

32. Identify any physical locations tied to the theft of trade secret, such as where it may be currently stored or used.

33. If you have conducted an internal investigation into the theft or counterfeiting activities, please describe any evidence acquired:

Civil Enforcement Proceedings

34. Has a civil enforcement action been filed against the suspects identified above? ___YES ___NO

a. If so, identify the following:

i. Name of court and case number:

ii. Date of filing:

iii. Names of attorneys:

iv. Status of case:

b. If not, is a civil action contemplated? What type and when?

35. Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

LAW ENFORCEMENT CONTACTS IN YOUR AREA: