EXHIBIT W

STATE OF MINNESOTA

IN DISTRICT COURT

COUNTY OF HENNEPIN

FOURTH JUDICIAL DISTRICT
Case Number: 27-CV-12-20976
Case Type: Civil

Guava LLC,

Plaintiff,

vs.

Spencer Merkel,

Defendant

AFFIDAVIT OF SPENCER MERKEL

STATE OF OREGON)
) ss.
COUNTY OF Washington)

SPENCER MERKEL, being first duly sworn under oath, deposes and states:

1. I am a resident of the State of Oregon. My address is [redacted]

1. I received a letter, dated September 26, 2012, from Prenda Law Firm regarding Hard Drive Productions, Inc. v. John Does 1-1,495. This letter stated that my IP address was observed distributing a movie called *Amateur Allure – MaeLynn*. The same letter offered me an opportunity to settle the case against me for a sum of money, and gave me less than two weeks (by the time I received the letter) in which to consider the offer. A copy of this letter is attached to this affidavit as Exhibit A.

2. Prior to the deadline I contacted Prenda Law and spoke with a gentleman named Mike or Michael. I informed Michael that I had downloaded the movie in question and asked about how I could settle this as I could not afford the settlement payment offered in the letter.

3. Michael offered me a settlement deal. The deal consisted of the following parts:

a. I would agree to be sued.

b. Prenda would ask for, and I would provide, a copy of the bit-torrent log from my computer. The excuse for gathering this log is that it would corroborate the IP address evidence that they had already gathered through the use of Prenda's software.

c. Prenda would, upon receipt of the information, dismiss the case against me.

4. In discussion of the settlement, Michael stated that he did not know of any pro bono attorneys in Oregon, but could provide the name of an attorney who might take my case in Minnesota. Because I cannot afford to pay an attorney, I agreed to be sued in the state of Minnesota. I then retained my attorney, Trina Morrison, based on the information provided to me by Prenda Law.

5. Before the start of this case, I had not heard of Guava LLC. I believed that I would be sued by Hard Drive Productions, Inc. I believe that Guava LLC's case against me is based on my admission to Michael that I downloaded the video at issue in the Hard Drive Productions case.

6. Before the case against me was filed, I had not heard of Alpha Law Firm. I believed that opposing counsel was Prenda Law.

7. After subpoenas were served in the case against me, I learned of Guava LLC's and Prenda Law's practice of finding one John Doe to be a named defendant, and then discovering the names of and requesting settlement money from other John Does by issuing subpoenas to ISPs.

8. Last week, on 01/15/13, I was once again contacted by Prenda Law Firm. I received a voice mail from someone on behalf of Prenda Law stating that I needed to make payment arrangements or I would be sued.

9. As of January 23, 2013, Guava LLC has not requested either the bit-torrent log from my computer or the names of any co-conspirators from me.

10. The Hard Drive Productions, Inc. movie that I admitted to downloading was downloaded from the now-defunct website www.cheggit.com. This website operated on a membership-basis that was, when I joined, free and open to anyone who was interested in joining.

11. I do not know the names, addresses, phone numbers, IP addresses, or email addresses of any other users of the website www.cheggit.com.

FURTHER YOUR AFFIANT SAYETH NOT.

Spencer Merkel

Subscribed and sworn to before me
this 24th day of January, 2013.

Notary Public

OFFICIAL SEAL
JANET L PARK
NOTARY PUBLIC-OREGON
COMMISSION NO. 462459
MY COMMISSION EXPIRES OCT. 13, 2015

Prenda Law Inc.
Intellectual Property Attorneys

VIA U.S. MAIL on 09/26/2012
Spencer Merkel
[redacted]

Re: Hard Drive Productions, Inc. v. John Does 1-1,495
1:11-cv-01741-JDB Ref #66261

Dear Spencer Merkel:

Prenda Law has been retained by Hard Drive Productions, Inc. to file lawsuits against people caught stealing its movies. Our client's engineers observed a user of your IP address illegally downloading its movie, ***Amateur Allure - MaeLynn***. This movie is protected by the United States Copyright Act.

In response to a subpoena issued in connection with a federal lawsuit, your Internet Service Provider, Comcast Cable Communications, identified you as the account holder. Specifically, Comcast Cable Communications identified you as the account holder of IP address 24.21.226.72 at the exact time of the infringement, which occurred at July 6, 2011 at 13:33:41 UTC.

Our client's forensic experts deploy sophisticated computer software to capture illegal downloading activities. These experts execute a comprehensive process to detect, record, monitor, verify and report infringing activity. The evidence collected by the forensic team is carefully maintained for future use at trial. A study published by the University of Colorado—and funded by Comcast and Time Warner—determined that the software technology utilized by our client's forensic experts authoritatively established that your IP address, 24.21.226.72, was observed illegally distributing ***Amateur Allure - MaeLynn*** at July 6, 2011 at 13:33:41 UTC. The study can be found at *http://cseweb.ucsd.edu/~dlmccoy/papers/bauer-wifs09.pdf*. The forensic experts preserved a piece of the file that the user of your IP address distributed to the other infringers, along with related evidence connected to your Internet account. The purpose of obtaining and preserving this data is so that our client is able to establish its allegations in court, if necessary.

Under the United States Copyright Act, copyright owners may recover up to $150,000 in statutory damages per infringing file, plus attorney's fees. In a Minnesota case very similar to this case, IP address account holder, Jamie Thomas-Rasset rejected an intial settlement offer and chose to litigate her case through trial. At trial, Ms. Thomas-Rasset argued that someone else used her account to commit infringement. The jury disregarded Ms. Thomas-Rasset's defense and awarded the copyright owner $222,000 in damages. A complete description of the case is available online at *http://en.wikipedia.org/wiki/Capitol_v._Thomas*.

In a Massachusetts case, an infringer named Joel Tennenbaum was accused of infringing several music files. Mr. Tennenbaum was offered a settlement of $3,500 for his infringing activities, which he rejected. The record companies secured a judgment in the amount of $675,000 against him. A complete description of the case is available online at *http://en.wikipedia.org/wiki/Sony_BMG_v._Tenenbaum.*

As with Ms. Thomas-Rasset and Mr. Tennenbaum, you have an opportunity to resolve this matter now. You will be able to put this matter behind you, avoid the stress of appearing as a defendant in a multi-year federal lawsuit, and the risk of a crippling jury verdict similar to those described above.

Our client has weighed several aspects of this case, including its likelihood of success, its likely recovery of damages, its attorney's fees award, and the extreme burden of federal litigation on all parties. In exchange for a comprehensive release of all legal claims in this matter, which will enable you to avoid becoming a named defendant in a lawsuit, our firm is authorized to accept the sum of $3,400.00 as full settlement for the claims. This offer will expire on 10/11/2012 at 4:00 p.m. CST.

Under the applicable rules of civil procedure, our lawsuit against you personally will not commence unless we serve you with a complaint. In the event we fail to come to a settlement, our client intends to proceed with sending your file to our local counsel in Beaverton and directing them to file a lawsuit.

To reiterate: If you act promptly, you will avoid being named as a defendant in a lawsuit. You may pay the settlement amount by:

(a) Mailing a check or money order payable to "Prenda Law Inc. Trust Account" to:

Prenda Law, Inc.
26298 Network Place
Chicago, IL 60673;

(b) Completing and faxing the enclosed payment authorization to **(312) 893-5677.**

It is very important to include your five digit reference number on your method of payment. Regardless of your payment method, once we have processed the settlement, we will send you your signed Release as confirmation that your payment has been processed and that our client's claims have been released.

Please consider this letter to constitute formal notice that until and unless we are able to settle our client's claim against you, we demand that you not delete any files from your computer or any other computers under your control or in your possession. If forced to proceed against you in a lawsuit, we will have a computer forensic expert inspect these computers in an effort to locate the subject content and to determine if you have deleted any content. If in the course of litigation, the forensic computer evidence suggests that you deleted media files, our client will amend its complaint to add a "spoliation of evidence" claim against you. Be advised that if we prevail on this additional claim, the court could award monetary sanctions, evidentiary sanctions and reasonable attorneys' fees. If you are unfamiliar with the nature of this claim in this context, please consult an intellectual property attorney.

We strongly encourage you to consult with an attorney to review your rights in connection with this matter. Although we have endeavored to provide you with accurate information, our interests are directly adverse to yours. You should not rely on the information provided in this letter for assessing your position in this case. Only an attorney who represents you can be relied upon for a comprehensive analysis of our client's claim against you. Due to the very special laws regarding intellectual property, we encourage you to consider consulting an attorney who is knowledgeable in this complicated area of federal law. This is particularly important if you decide to litigate this matter. If in fact you do wish to move forward with litigation but do not have an attorney, the OR state bar has an attorney referral service you may wish to contact.

However, If you wish to settle the matter, our office has enclosed a payment authorization form along with a sample of the Release that you will receive after settlement. We look forward to resolving our client's claim against you in an amicable fashion, through settlement, if possible.

Sincerely,

Paul Duffy
Attorney and Counselor at Law
Licensed in Illinois, California,
Massachusetts, and the District of Columbia
Enclosures

Legal Correspondence Settlement Purposes Only Not Admissible Under FRE 408

Prenda Law Inc.
Protecting Intellectual Property

PAYMENT AUTHORIZATION

I hereby authorize Prenda Law Inc. to withdraw funds from the bank account or credit card listed below for the settlement amount and legal issue referred to on my Release and herein below.

Case Name and Ref#: _____

PAYOR INFORMATION

Payor's Name: _____

Billing Address: _____

_____

Telephone Number: _____

Signature: _____ Date: _____

PAYMENT INFORMATION

Payment amount: $_____

Name on Bank Account / Credit Card: _____

If paying via bank account:

Type of Account: Checking / Savings

Routing Number: _____ Account Number: _____

If paying via credit card:

Card Number: _____ Exp. Date: _____

Card Type: ☐ Master Card ☐ Visa ☐ AmEx ☐ Discover

CID Number: _____ (this is the last three digits on the back of your Master Card, Visa, or Discover Card, or the four digit number in the upper right corner on the front of your AmEx)

Fax or mail this authorization to:

Prenda Law Inc.
26298 Network Place
Chicago, IL 60673

Fax: (312) 893-5677

IN RE: «Case», «CaseNo»
Title of Work: «PiratedContent»

CONDITIONAL RELEASE AND SETTLEMENT AGREEMENT

THIS SETTLEMENT AGREEMENT (the "Agreement") is entered into as of «Letter1_Expiration» ("Effective Date"), by and between «Client», ("Owner" or "Plaintiff") and the individual or entity that was assigned IP Address «IP_Address» on «Dday» (UTC), by «ISP» (the "Subscriber" or "Defendant John Doe") (Owner and Subscriber are collectively the "Parties").

NOW, THEREFORE, in consideration of the mutual promises contained herein and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Settlement Money. Subscriber shall pay Owner the sum of «Settlement» (the "Settlement Money"). The Settlement Money shall be tendered in the form of a cashier's check, credit card or law firm check with no charge back or check cancellation, made payable to the order of "Prenda Law Inc." and delivered to Prenda Law Inc. 26298 Network Place, Chicago, IL 60673. Subscriber's payment, and Owner's receipt, of the Settlement Money shall be a condition precedent to Owner's obligation under this Agreement, as set forth below, to voluntarily dismiss with prejudice its claims against the Subscriber in the above referenced law suit.

2. Confidentiality – Non Admission. The terms of this Agreement shall be kept confidential. Notwithstanding the foregoing, in the event of any legal action or proceeding or requirement under applicable law or government regulations compelling disclosure of this Agreement or the terms hereof, the recipient shall forthwith notify the other party in writing of such request so that the other party may seek an appropriate protective order or take other protective measures. If, in the absence of a protective order, the recipient is liability. This Agreement is the result of a compromise and shall not be construed as an admission by the Parties of any liability, wrongdoing, or responsibility on their part or on the part of their predecessors, successors, parents, subsidiaries, affiliates, attorneys, officers, directors or employees. Indeed, the Parties expressly deny any such liability, wrongdoing or responsibility.

3. Mutual Releases.
   a. **Owner** and their agents, principals, attorneys, heirs, executors, administrators, predecessors, successors, assigns and privies (the "Owner Releasors"), hereby remise, release, and forever discharge Subscriber, and all of their agents, principals, partners, officers, directors, employees, associates, attorneys, insurers, heirs, executors, administrators, predecessors, successors, affiliated entities, assigns, privies, spouses and all other persons, firms or corporations, which are or might be claimed to be liable (the "Subscriber Released Parties") by virtue of the Subscriber Released Parties' liability for uploading, downloading or otherwise infringing upon Owner's copyright of the "Work", which the Owner Releasors, now have or ever had against the Subscriber Released Parties for any act or omission occurring up to and including the date of this Agreement. The Owner Releasors recognize and understand that they are releasing the aforementioned liability for any act or omission occurring up to and including the date of this Agreement which relates to the Work, regardless of whether or not they knew of said act, omission or of any injury relating thereto.
   b. **Subscriber** and their agents, principals, partners, officers, directors, employees, associates, attorneys, insurers, heirs, executors, administrators, predecessors, successors, affiliates entitles, assigns, privies, spouses and all other persons, firms or corporation, which are or might be claimed through them (the "Subscriber Releasors"), hereby remise, release, and forever discharge Owner and all of their agents, principals, partners, officers, directors, employees, associates, attorneys, insurers, heirs, family members, executors, administrators, predecessors, successors, affiliated entities, assigns, privies, spouses and all other persons, firms or corporations, which are or might be claimed to be liable (the "Owner Released Parties") by virtue of the owner Released Parties' liability, for any and all actions relating to Owner's conduct in instituting the lawsuit first referenced above in which the Subscriber Releasors, not have or ever had against the Owner Released Parties. The Subscriber Releasors recognize and understand that they are releasing the aforementioned liability for any act or omission occurring from the beginning of time up to and including the date of this Agreement, regardless of whether or not they knew of said act, omission or of any injury relating thereto.

4. Independent Counsel. Each party acknowledges that is has read, reviewed, and fully considered the terms of this Agreement, has had the opportunity to consult with legal counsel, has made such investigation of facts pertinent hereto as it deems necessary and appropriate, and fully understands the terms and effect of this Agreement and executes the same freely of its own accord.

5. No Admission of Liability. The Parties have determined that is would be in their mutual best interests not to engage in further litigation and desire to amicably resolve this matter. It is understood and agreed that this settlement is the compromise of a disputed claim, and that the payment made and other performances hereunder are not to be construed

as admissions of liability on the part of the party or parties hereby released and that the parties deny liability and intend merely to avoid litigations and buy their peace.

6. Venue. The venue for any action seeking to enforce or construe the meaning of this Agreement or the obligations of the Parties here under shall be the United States District Court for the Southern District of Florida.

7. Legal Fees and Costs. Each party shall be responsible for paying its respective legal expenses and costs incurred in connections herewith and no moneys will be exchanged except as otherwise provided for herein. Should it become necessary for either party to institute legal action to enforce the terms of this Agreement the prevailing party shall be entitled to recover from the other party the reasonable attorneys' fees and costs associated with any such actions.

8. Binding Effect. This Agreement shall inure to the benefit of and be binding upon the parties hereto and to their respective successors and legal representatives.

9. Nonwaiver. No provision of this Agreement shall be adjudged waived unless any such waiver is signed by the party against whom the waiver is asserted. The waiver by any party of a breach of any provision of this Agreement shall not operate or be construed as a waiver of any subsequent breach.

10. Severability. If any provisions or application of this Agreement shall be held invalid or unenforceable then any such provisions shall be deemed severed from this Agreement and the remaining provisions and applications of this Agreement shall not be affected, but rather shall remain valid and enforceable.

11. Entire Agreement. This Agreement constitutes the entire agreement and supersedes any and all other understandings and agreements between the parties with respect to the subject matter hereof and no representation, statement or promised not contained herein shall be binding on either party. This Agreement may be modified only by a written amendment duly signed by each party.

12. Successors and Assigns. This Agreement shall be binding on and inure to the benefit of all parent companies, affiliates, subsidiaries, related companies, defendants, franchisees, successors and assigns of each of the parties hereto.

13. Jointly Drafted. The parties to this Agreement have cooperated in the drafting and preparation of this Agreement. Therefore, this Agreement shall not be construed against either party on the basis that they independently drafted this Agreement.

Authority. Each of the undersigned signatories hereby represents and warrants that he or she has the authority to bind the individual or entity on whose behalf he or she is signing this Agreement.

IN WITNESS WHEREOF,

_____

Paul A. Duffy
Prenda Law Inc.
Counsel for Plaintiff

EXHIBIT X

Guava LLC

2100 M STREET NORTHWEST | SUITE 170-417 | WASHINGTON DC | 20037
P 888-568-WIRE (9473) | F 888-964-WIRE (9473)

01/30/2013
SENT VIA U.S. MAIL
[redacted]

Re: Guava LLC v. Comcast Cable Communications LLC
12-MR-417 Ref #[redacted]

Dear [redacted]

This letter is to provide you legal notice that a lawsuit involving you has been filed in St. Clair County, Illinois. The case, Guava LLC v. Comcast Cable Communications, LLC, was filed on November 20, 2012 in the Circuit Court of the Twentieth Judicial Circuit, St. Clair County, Illinois Law Division. The purpose of this letter is to put you on notice of impending litigation and allow you the opportunity to seek legal counsel or speak with someone from our office regarding this matter.

Our company, Guava LLC, operates computer systems on behalf of our clients, who are adult content producers. Our computers were breached and our files were stolen. Our engineers observed your Internet account distributing these files via BitTorrent. BitTorrent is associated with such websites and software as the Pirate Bay and Transmission. For more information regarding BitTorrent you may reference online sources.

In the course of discovery, we issued subpoenas to various Internet Service Providers (ISPs) to obtain the identifying information of the wrongdoers. On November [redacted] 2012 [redacted] UTC, our engineers observed your IP address, [redacted], trading in the files that were taken from our company's computers. Your ISP, Comcast, turned over records confirming that you were the account holder of IP [redacted] on the date in question. Based on this information, we will seek to hold you (or the person who used your Internet account) liable for this conduct. For your reference, we have enclosed a copy of the petition that was filed in this lawsuit. Please understand that if we are forced to proceed against you individually for the acts we observed your subscriber account committing, the actual complaint naming you as a defendant could possibly include additional counts, depending on what violations were observed.

Under the applicable rules of civil procedure, our lawsuit against you personally will not commence unless we serve you with a complaint. Please consider this letter to constitute formal notice that we demand that you not delete any files from your computer or any other devices under your control or in your possession. You have an affirmative obligation to preserve evidence, including router logs and computer files. A failure to do so may subject you to additional liability. You should consult an attorney to understand your obligations in this regard.

Many account holders contact our company to find out more about our claims or to resolve them before we refer this matter to our attorneys. While we certainly are willing to discuss resolution, we are also preparing to litigate this matter in the event a resolution is not reached. We have found that the earlier we are able to reach a resolution, the less expensive it is for both you and our company. As time passes, we (and you) will incur attorney's fees and court costs. The amount for which would be willing to resolve this matter for today will increase over time in proportion to the fees and expenses we incur.

As you know, being named as a defendant in a lawsuit can be time-consuming, distressing and expensive. Although we have endeavored to provide you with accurate information, our interests are directly adverse to yours and you should not rely on the information provided in this letter for assessing your position in this case. Only an attorney who represents you can be relied upon for a comprehensive analysis of our company's claims. Our records indicate that you are not represented by an attorney. If you are represented by an attorney please forward this letter to him or her and have your attorney contact our office immediately to indicate their representation.

PLEASE BE ON NOTICE: Due to the serious nature of this matter, we are referring this matter to our attorneys for further prosecution against you in 21 days if we do not hear from you.

Sincerely,

Brett Gibbs
In-House Counsel, Guava LLC
Licensed only in the state of California.

Notice of Offer of Settlement

Formal Date of Offer: 01/31/2013

Pursuant to our obligation to attempt to resolve our legal claims prior to filing a lawsuit against you personally, we hereby provide you the following settlement offer. If you reject our offer, or we do not hear from you within 21 days of the date of this letter, we will direct our attorneys to file a lawsuit against you personally. We believe that due to several factors, including our good faith offer to settle at this early stage of the case, we would be entitled to full damages.

We have weighed several aspects of this case, including our likelihood of success, our likely recovery of damages, the availability of an attorney's fees award, and the extreme burden of litigation on all parties. In exchange for a comprehensive release of all legal claims in this matter, which will enable you to avoid becoming a named defendant in a lawsuit, we will accept the sum of $4,000.00 as full settlement for our claims. This offer will expire in 21 days at 4:00 p.m. CST.

To reiterate: If you act promptly, you will avoid being named as a defendant in a lawsuit. You may pay the settlement amount by:

(a) Mailing a check or money order payable to "Guava LLC" to:
Guava LLC
2100 M Street Northwest, Suite 170-417
Washington DC, 20037-1233

(b) Completing and faxing the enclosed payment authorization to
1-888-964-9473.

It is very important to include your five digit reference number on your method of payment. Regardless of your payment method, once we have processed the settlement, we will send you your signed Release as confirmation that your payment has been processed and that our company's claims have been released.

Our records indicate that you are not represented by an attorney. If you are represented by an attorney please forward this offer of settlement to your attorney and have your attorney contact our office immediately to indicate their representation.

Guava LLC

2100 M STREET NORTHWEST | SUITE 170-417 | WASHINGTON DC | 20037
P 888-588 WIRE (9473) | F 888-964 WIRE (9473)

PAYMENT AUTHORIZATION

I hereby authorize Guava, LLC to withdraw funds from the bank account or credit card listed below for the settlement amount and legal issue referred to on my Release and herein below.

Case Name and Reference #: _____

PAYOR INFORMATION

Payor's Name: _____

Billing Address: _____

_____

Telephone Number: _____ Email address: _____

Signature: _____ Date: _____

_____

PAYMENT INFORMATION

Payment amount: $ _____

Name on Bank Account / Credit Card: _____

If paying via bank account:

Type of Account: Checking / Savings

Routing Number: _____ Account Number: _____

If paying via credit or debit card:

Card Number: _____ Exp. Date: _____

Card Type: ☐ Master Card ☐ Visa ☐ AmEx ☐ Discover

CID Number: _____ (this is the last three digits on the back of your Master Card, Visa, or Discover Card, or the four digit number in the upper right corner on the front of your AmEx)

Fax, scan & email, or mail this authorization to:

Guava, LLC
2100 M Street Northwest, Suite 170-417
Washington, DC 20037
Fax: 888.964.WIRE (9473)
email: accounting@livewireholdings.com

www.livewireholdings.com

IN THE CIRCUIT COURT OF THE TWENTIETH JUDICIAL CIRCUIT
ST. CLAIR COUNTY, ILLINOIS

GUAVA LLC,

Petitioner,

v.

COMCAST CABLE COMMUNICATIONS, LLC,

Respondent.

No. 12-MR-417

FILED
ST. CLAIR COUNTY
DEC 12 2012
22
CIRCUIT CLERK

ORDER GRANTING PETITION FOR DISCOVERY BEFORE SUIT TO IDENTIFY RESPONSIBLE PERSONS AND ENTITIES AND DENYING RESPONDENT'S MOTION TO DISMISS

THIS CAUSE, having come before this Court on Petitioner's Petition for Discovery before Suit to Identify Responsible Persons and Entities ("Petition") and Respondent's Motion to Dismiss, and the Court having reviewed said Petition, the Memorandum of Law filed in support thereof, and Respondent's Motion to Dismiss; the parties are present through counsel; the Court having heard argument and being otherwise duly advised in the premises, hereby makes the following:

FINDINGS OF FACT

1. Petitioner alleges that the identifying information of Respondent's subscribers and the forensic information contained on the subscribers' computers is under an imminent threat of permanent destruction.

2. Although Respondent has the ability to preserve the identifying information of its subscribers, it has no control over the forensic information stored on its subscriber's computers.

3. Petitioner alleges that this forensic information consists, *inter alia*, of computer logs that are stored exclusively on the Doe Defendant's computers. The computer logs are electronic files that are subject to being overwritten, deleted or modified.

4. Petitioner alleges that the computer logs contain information that will be necessary for Petitioner to prove its underlying case.

5. Petitioner alleges that if this information is destroyed, Petitioner will have no means of bringing suit against individuals who allegedly hacked into Petitioner's computer systems.

6. Petitioner alleges that any delay in providing Petitioner with the identifying information of Respondent's subscribers will irreparably harm Petitioner.

IT IS ORDERED AND ADJUDGED as follows:

1. Respondent's Motion to Dismiss is DENIED and Petitioner's Rule 224 Petition is GRANTED.

2. Respondent shall provide any affected subscribers with a copy of Petitioner's Petition and a copy of this Order on or before December 26, 2012.

3. Any subscriber seeking to file an Objection or a Motion to Quash, Dismiss or Sever, must do so by filing said pleading with the Clerk of the Circuit Court, St. Clair County, Illinois, on or before January 25, 2013.

4. Except as to those subscribers who file a timely pleading as described in paragraph 3 above, Respondent shall provide Petitioner with the true name, address, telephone number, e-mail address, Media Access Control ("MAC") address for each of the John Does ("Does") to whom Respondent assigned an Internet Protocol ("IP") address as set forth on Exhibit A to the Petition on or before January 30, 2013, except for the IP addresses for which Respondent has no identifying information, as long as Respondent identifies said IP addresses.

5. If a subscriber files an Objection, Motion to Quash, Dismiss or Sever, Respondent shall withhold the identifying information associated with that particular subscriber, pending resolution by the Court as set forth below.

6. All Objections, Motions to Quash, Dismiss or Sever shall be set for hearing on February 13, 2013 at 9:00 A.M. before the Honorable Andrew J. Gleeson in Courtroom 404, St. Clair County Building, Belleville, Illinois.

7. Petitioner shall pay Respondent's reasonable costs in identifying and notifying its subscribers under the terms of this Order. If necessary, the Court shall resolve any disputes between Respondent and Petitioner regarding the reasonableness of the amount proposed to be charged by Respondent after the information is provided to Petitioner.

Entered this 12th day of December, 2012.

Andrew J. Gleeson
Circuit Judge

FILED
ST. CLAIR COUNTY
DEC 12 2012
22 CIRCUIT CLERK

EXHIBIT Y

Prenda Law Inc.
Protecting Intellectual Property

November 18, 2012

Paul A. Duffy
Prenda Law, Inc.
161 N. Clark St. Ste 3200
Chicago, IL 60601

Honorable Judge Mary S. Scriven
U.S. District Court for the Middle District of Florida
Sam M. Gibbons U.S. Courthouse
801 North Florida Ave.
Tampa, FL 33602

Re: Order at Dkt. 17 in Case no. 8:12-cv-01685-MSS-MAP

Dear Judge Scriven:

I have very recently been made aware that the Court ordered "a principal of Prenda Law, Inc." to appear in person at a motion to dismiss hearing scheduled for November 27, 2012 in case number 8:12-cv-01685-MSS-MAP. (Dkt. 17.) As the sole principal of Prenda Law, Inc. ("Prenda"), that would be me. For the record, I was never served with notice of the Court's order or otherwise made aware of it---until very recently via a phone call from a fellow attorney.

As an initial matter, I must respectfully inform the Court that I am located in Chicago, Illinois and my attendance at the hearing would require air travel. Due to a recent surgery on my eye, my doctor has ordered me not to travel by air due to the high risk of catastrophic injury or death due to changes in air pressure. I will be pleased to provide the Court with a surgeon's note upon request. Further, on November 27, 2012, I have three status hearings at 10:00 a.m. (EST) scheduled in the U.S. District Court for the Northern District of Illinois.

I also respectfully question how my appearance could benefit the Court, particularly since I am not representing *anyone* in this case and have no authority to speak on anyone's behalf. It would clearly be improper for me to make any statement in a matter pending in a jurisdiction in which I am not licensed and on behalf of a client that I do not represent.

In light of the foregoing statements, I pray that the Court will excuse my attendance at the November 27, 2012 hearing.

cc: Counsel of Record (via e-mail)

Sincerely,

Paul A. Duffy, Esq

EXHIBIT Z

MENU

Founding Partner Paul Duffy
Nationwide Attorney Network

Paul A. Duffy, J.D.

For more than 20 years, Mr. Duffy has been fighting to protect his client's intellectual property rights. He represents the interests of clients before federal district and state courts involving complex consumer fraud, copyright infringement analysis and prosecution, licensing rights, sharing agreements, trademark infringement analysis and prosecution, and website hacking prosecution.

Mr. Duffy and the other intellectual property attorneys of Prenda Law Inc. have been leading a nationwide revolution against internet piracy. He has experience with both prosecution and defense which gives him the ability to see a case from both perspectives. Mr. Duffy's extensive technical background, along with his dedication to comprehensive research and innovative thinking has enabled Prenda Law Inc. to become one of the leading intellectual property law firms in the United States today.

EDUCATION

Mr. Duffy received his law degree (J.D.) from the DePaul University College of Law, and his Bachelor of Science (B.S.) in Chemistry with a minor in Physics and Mathematics from Elmhurst College.

ADMISSIONS AND REGISTRATIONS

State of Illinois
U.S. District Court for each of the Northern, Central and Southern Districts of Illinois

State of California
U.S. District Court for the Southern District of California

Commonwealth of Massachusetts
U.S. District Court for the District of Massachusetts

District of Columbia
U.S. District Court for the District of Columbia

Professional Career

- Freeborn & Peters, attorney and partner
- Winston & Strawn, attorney and partner
- Waste Management, environmental engineering
- Commonwealth Edison Co., environmental and nuclear engineering

COMMUNITY SERVICE

Mr. Duffy provides pro bono services to three local organizations: the Heartland Alliance, Chicago Volunteer Legal Services, and the Center for Elder and Disability Law.

PRENDA LAW INC. INTELLECTUAL PROPERTY ATTORNEYS BLOG

Please visit our blog to find out about the lastest in the anti-piracy wars.

THE BLOG

PRENDA LAW INC.
Intellectual Property Attorneys

[redacted]Home | About the Firm | Firm Resources | Attorneys | Practice Areas | Giving | Case Samples | Terms of Service

EXHIBIT AA

John Steele

3rd

Of Counsel to Various Intellectual Property Firms

Greater Chicago Area | Law Practice

Current Various Law Firms
Previous Steele Hansmeier PLLC, Steele Law Firm, Bear Education
Education Georgetown University

Connect | Send InMail

269 connections

www.linkedin.com/in/thepirateslayer/ Contact Info

BACKGROUND

SUMMARY

I defend and protect copyright works. Working with law firms and companies across the country, I help pursue those intent on stealing copyrighted works on the internet (i.e. "pirates").

My practice, and the work I pioneered has been in over three hundred newspapers and I am regularly involved in litigation before federal appellate courts and state supreme courts.

My goal is to be hated by pirates, loved by clients, and to enjoy the wonderful life god has given me.

Specialties: Copyright Infringement.

EXPERIENCE

Of Counsel
Various Law Firms
November 2011 – Present (1 year 4 months) | Everywhere

If you are reading this, you probably know exactly what I do.

Founding Attorney
Steele Hansmeier PLLC
January 2009 – November 2011 (2 years 11 months) | Chicago

Pioneered the concept of going after people who steal copyrighted works on the internet. Sold client book to Prenda Law in 2011 and now assist attorneys throughout the country in fighting illegal infringement on the internet.

Founding Attorney
Steele Law Firm
July 2007 – January 2010 (2 years 7 months) | Chicago

Founding attorney at Steele Law Firm, a Chicagoland law firm focusing on Family Law matters including divorce, child support, child custody, adoption, and bankruptcy.

President
Bear Education
January 1999 – April 2005 (6 years 4 months)

Managed multiple vocational schools dedicated to computer engineering and network engineering oriented professions.

PEOPLE SIMILAR TO JOHN

Jenn Spears 3rd
Attorney at Martson Law Offices
Connect

PEOPLE ALSO VIEWED

Paul Hansmeier
Partner at Alpha Law Firm LLC

Brett Gibbs
Attorney

Nathan Wersal
Legal Research & Writing

Sirh Ryun Stella Dugas
Associate

Show Wang
Law Student

Valerie Wright
Student at Wheaton College

Chris Knowles
Sales at Unishippers

Jeff Glock
--

Jeffrey Powers
Checkpoint World Team Inc

Coby Cathey
Owner, Resolute Academy

Built and sold laptop computer equipment. Trained people in computer networking.

SKILLS & EXPERTISE

Catching those who...

EDUCATION

Georgetown University
BA
Activities and Societies: Magna Cum Laude Phi Beta Kappa

University of Minnesota Law School
JD

RECOMMENDATIONS Given (1)

Bruce Beddard
Vice President

"Bruce is a great mortgage consultant who works hard to help people understand not only their mortgage needs, but issues relating to mortgages such as credit scoring, and FHA loans.

Bruce is also an excellent basketball player!

January 15, 2009, John was with another company when working with Bruce at mTeam Mortgage Group

SEE MORE

GROUPS

HAPPY LAWYERs 8... Join
Imerman Angels Join
Link to Chicago Join
Linked N Chicago (Li... Join
Solo Attorney Practit... Join
e-LEGAL Join

FOLLOWING


You


Mike O'Horo


Andrew Bleiman

Your connections can introduce you to someone who knows John
Get introduced


John Steele

IN COMMON WITH JOHN

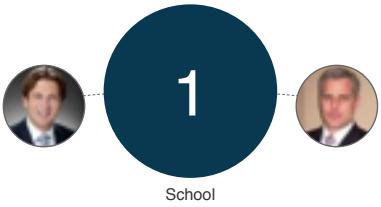


EXHIBIT BB

STATE OF MINNESOTA

IN DISTRICT COURT

COUNTY OF HENNEPIN

FOURTH JUDICIAL DISTRICT
Case Type: Civil

GUAVA LLC,

Plaintiff,

vs.

SPENCER MERKEL,

Defendant.

Court File No.
Judge:

SUMMONS

THIS SUMMONS IS DIRECTED TO SPENCER MERKEL.

1. **YOU ARE BEING SUED**. The Plaintiff has started a lawsuit against you. The Plaintiff's Complaint against you is attached to this summons. Do not throw these papers away. They are official papers that affect your rights. You must respond to this lawsuit even though it may not yet be filed with the Court and there may be no court file number on this summons.

2. **YOU MUST REPLY WITHIN 20 DAYS TO PROTECT YOUR RIGHTS**. You must give or mail to the person who signed this summons **a written response** called an Answer within 20 days of the date on which you received this Summons. You must send a copy of your Answer to the person who signed this summons located at:

Michael K. Dugas
Alpha Law Firm LLC
900 IDS Center
80 South 8th Street
Minneapolis, MN 55402

3. **YOU MUST RESPOND TO EACH CLAIM.** The Answer is your written response to the Plaintiff's Complaint. In your Answer you must state whether you agree or disagree with each paragraph of the Complaint. If you believe the Plaintiff should not be given everything asked for in the Complaint, you must say so in your Answer.

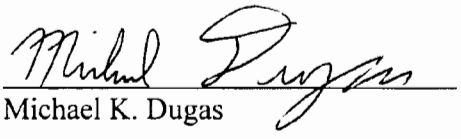
4. YOU WILL LOSE YOUR CASE IF YOU DO NOT SEND A WRITTEN RESPONSE TO THE COMPLAINT TO THE PERSON WHO SIGNED THIS SUMMONS. If you do not Answer within 20 days, you will lose this case. You will not get to

tell your side of the story, and the Court may decide against you and award the Plaintiff everything asked for in the complaint. If you do not want to contest the claims stated in the complaint, you do not need to respond. A default judgment can then be entered against you for the relief requested in the complaint.

5. LEGAL ASSISTANCE. You may wish to get legal help from a lawyer. If you do not have a lawyer, the Court Administrator may have information about places where you can get legal assistance. **Even if you cannot get legal help, you must still provide a written Answer to protect your rights or you may lose the case.**

6. ALTERNATIVE DISPUTE RESOLUTION. The parties may agree to or be ordered to participate in an alternative dispute resolution process under Rule 114 of the Minnesota General Rules of Practice. You must still send your written response to the Complaint even if you expect to use alternative means of resolving this dispute.

DATED: October 15, 2012

By: 
Michael K. Dugas

STATE OF MINNESOTA
COUNTY OF HENNEPIN

IN DISTRICT COURT
FOURTH JUDICIAL DISTRICT
Case Type: Civil

GUAVA LLC,

Plaintiff,

vs.

SPENCER MERKEL,

Defendant.

Court File No.
Judge:

COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Guava LLC, by and through its undersigned counsel, hereby files this Complaint requesting damages and injunctive relief, and alleges as follows:

INTRODUCTION

1. Plaintiff files this action for interception of electronic communications and civil conspiracy, arising from unlawful computer breaches. By this action, Guava seeks compensatory damages, injunctive relief and attorney's fees and costs.

PARTIES

2. Plaintiff is a limited liability company that owns and operates protected computer systems, including computer systems accessible throughout Minnesota.

3. Defendant Spencer Merkel breached Plaintiff's protected computer systems and intercepted Plaintiff's electronic communications.

BACKGROUND

4. Hacking has become a serious threat to anyone maintaining private or protected computer systems. *See* Kevin Parrish, *Hackers Have Access to 1 in 5 Microsoft Logins*, TOM'S GUIDE, July 16, 2012, attached hereto as Exhibit A (finding that "20-percent of

Microsoft Account logins are found on lists of compromised credentials stemming from hack attacks on other services like Yahoo and Facebook."); Michael Mimoso, *Cybercrime Gang Recruiting Botmasters for Large-Scale MiTM Attacks on American Banks*, THE THREAT POST, Oct. 4, 2012, attached hereto as Exhibit B (explaining that "[a]s many as 30 banks have been targeted" recently by cyber hackers.); Bryon Acohido, *No Slowdown in Sight for Cyberattacks*, USA TODAY, July 30, 2012, attached hereto as Exhibit C (Eddie Schwartz, chief security officer of security firm RSA stating that "[i]t's easier and safer for a criminal to steal money from an online bank account, rather than have to walk into a bank — or to steal intellectual property in an online setting, rather than have to send in a human spy.").

5. Even large corporations and governmental agencies are not immune from hacking attacks. *See* Kim Zetter, H*ackers Release 1 Million Apple Device IDs Allegedly Stolen From FBI Laptop*, WIRED, Sept. 4, 2012, attached hereto as Exhibit D (explaining that a hacker group obtained "1 million Apple device IDs that" were "obtained from an FBI computer they hacked.").

6. Companies harmed by hacking are encouraged to seek relief in the courts. *See* Glenn Chapman, *Cyber Defenders Urges to go on the Offense*, AMERICAN FREE PRESS, July 26, 2012, attached hereto as Exhibit E (former FBI cyber crime unit chief Shawn Henry explaining that "I believe the threat from computer network attack is the most significant threat we face as a civilized world, other than a weapon of mass destruction." and Black Hat founder Jeff Moss proposing that "cyber attackers also be fought on legal fronts, with companies taking suspected culprits to court.").

FACTUAL ALLEGATIONS

7. Plaintiff operates computer systems that distribute third-party content. By way of analogy, Plaintiff is like a satellite radio station in that it distributes content owned by others. Plaintiff generates revenue by requiring third-parties to pay a fee for accessing its distributions systems. Members are assigned a username and password in order to access the distribution system.

8. Defendant used a username and password that did not belong to him to gain unauthorized access to Plaintiff's protected computer systems. Once he gained unauthorized access to Plaintiff's protected computer systems he intercepted electronic communications between Plaintiff and its legitimate members.

9. Defendant obtained the username and password he used to gain unauthorized access to Plaintiff's protected computer systems from a website that allows its members to trade stolen usernames and passwords amongst one another.

COUNT I – INTERCEPTION OF ELECTRONIC COMMUNICATIONS

10. Plaintiff hereby incorporates by reference each and every allegation contained in the preceding paragraphs as if set forth fully herein.

11. Defendant used hacked usernames and passwords to gain access to Plaintiff's protected computer systems and intentionally intercepted numerous electronic communications between Plaintiff and its paying members.

12. The intercepted electronic communications included information regarding the identities of Plaintiff's customers, account information, financial information, computer programming and security information, and other information that Plaintiff protects and

does not even give access to third parties, even those who pay for and obtain legitimate passwords to access Plaintiff's websites.

13. Plaintiff has suffered actual damages as a result of Defendant's actions.

14. Defendant profited by the unauthorized interceptions of Plaintiff's electronic communications.

15. Those actions on the part of Defendant constitute violations of Minn. Stat. § 626A.02 Interception and Disclosure of Wire, Electronic, or Oral Communications Prohibited. A private right of action exists under Minn. Stat. § 626A.32.

COUNT II – CIVIL CONSPIRACY

16. Plaintiff hereby incorporates by reference each and every allegation contained in the preceding paragraphs as if set forth fully herein.

17. Defendant colluded with multiple members of a hacking community to intercept electronic communications taking place on Plaintiff's protected computer systems. The hacking community's members share hacked usernames and passwords among other members to ensure that they had access to Plaintiff's protected computer systems.

18. Defendant reached an agreement with his fellow co-conspirators to gain unlawful access to Plaintiff's computer systems and intercept electronic communications. Defendant was aware that the hacked username and password he used did not belong to him and that he did not have Plaintiff's permission to access its computer systems and electronic communications.

19. Defendant committed overt tortious and unlawful acts by using hacked usernames and passwords to impermissibly obtain access to Plaintiff's protected computer systems and electronic communications.

20. As a proximate result of this conspiracy, Plaintiff has been damaged, as is more fully alleged above.

JURY DEMAND

21. Plaintiff hereby demands a jury trial in this case.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays judgment and relief against Defendant as follows:

1) Judgment against Defendant that he or she has committed prohibited interception of Plaintiff's electronic communications pursuant to Minn. Stat. § 626A.02;

2) Judgment in favor of the Plaintiff against the Defendant for actual damages or statutory damages pursuant to Minn. Stat. § 626A.02 and common law, at the election of Plaintiff, in an amount in excess of $100,000 to be ascertained at trial;

3) On Count II, an order that Defendant is jointly and severally liable to the Plaintiff in the full amount of Judgment on the basis of a common law claim of civil conspiracy;

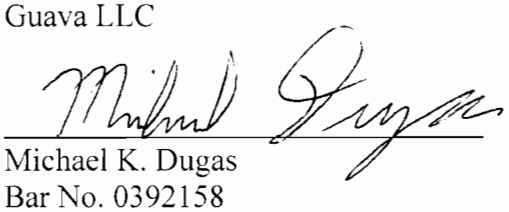
4) Judgment in favor of Plaintiff against the Defendant awarding the Plaintiff attorneys' fees, litigation expenses (including fees and costs of expert witnesses), and other costs of this action; and

5) Judgment in favor of the Plaintiff against Defendant, awarding Plaintiff declaratory and injunctive or other equitable relief as may be just and warranted.

Respectfully submitted,

Guava LLC

DATED: October 5, 2012

By: 

Michael K. Dugas
Bar No. 0392158
Alpha Law Firm LLC
900 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (415) 325 – 5900
mkdugas@wefightpiracy.com
Attorney for Plaintiff

EXHIBIT A

Hackers Have Access To 1 in 5 Microsoft Logins

9:00 PM - July 16, 2012 - By Kevin Parrish - Source : Microsoft

Microsoft blames the re-use of passwords for the high account hacking rate.

Zoom Eric Doerr, Group Program Manager for Microsoft's Account system, said on Sunday that 20-percent of Microsoft Account logins are found on lists of compromised credentials stemming from hack attacks on other services like Yahoo and Facebook. Naturally he slammed the use of providing the same passwords and login details across multiple services, saying that one breached service could mean multiple account hacks.

"These attacks shine a spotlight on the core issue – people reuse passwords between different websites," he said on Sunday. "This highlights the longstanding security advice to use unique passwords, as criminals have become increasingly sophisticated about taking a list of usernames and passwords from one service and then 'replaying' that list against other major account systems. When they find matching passwords they are able to spread their abuse beyond the original account system they attacked."

Doerr said that Microsoft regularly gets notified of lists of compromised external account info (email addresses and/or passwords from other networks) from different sources. These sources can include one of the many worldwide law enforcement agencies, an ISP, and even another company that runs an identity system. They contact Microsoft so that users are informed about a possible account hacking.

"You'd be surprised how often the lists – especially the publicly posted ones – are complete garbage with zero matches," Doerr said. "But sometimes there are hits – on average, we see successful password matches of around 20-percent of matching usernames. A recent one only had 4.5-percent overlap. This is actually exciting because it means that, on average, 80% of our customers are following safe password practices, and this reflects a growing sophistication in our customers."

He said when Microsoft receives a list, the company checks to see if it actually matches any accounts and passwords in the system through an automated hands-off process. Then the company looks to see if there is any evidence of criminal activity like sending spam. If there are signs of criminal activity, then the account is suspended until the owner goes through the recovery process.

"Occasionally we get information about a set of customers, but there isn't enough account information to identify who has reused passwords and is therefore at risk," he said. "Then we have a judgment call – do we ask 100-percent of those customers to reset their passwords, even though only 20-percent are probably at risk? Or do we leave the 20-percent at risk to avoid inconveniencing the 80-percent?"

Where there is a credible threat, Microsoft would rather inconvenience 100-percent of the customers by resetting all passwords, he said.

Currently the team is working on beefing up security by offering increased password lengths. "Unfortunately, for historical reasons, the password validation logic is decentralized across different products, so it's a bigger change than it should be and takes longer to get to market," he added. "It's also worth noting that the vast majority of compromised accounts are through malware and phishing. The small fraction of brute force is primarily common passwords like '123456' not due to a lack of complexity."

EXHIBIT B

October 4, 2012, 12:15PM

Cybercrime Gang Recruiting Botmasters for Large-Scale MiTM Attacks on American Banks

by Michael Mimoso

A slew of major American banks, some already stressed by a stream of DDoS attacks carried out over the past 10 days, may soon have to brace themselves for a large-scale coordinated attack bent on pulling off fraudulent wire transfers.

RSA's FraudAction research team has been monitoring underground chatter and has put together various clues to deduce that a cybercrime gang is actively recruiting up to 100 botmasters to participate in a complicated man-in-the-middle hijacking scam using a variant of the proprietary Gozi Trojan.

This is the first time a private cybercrime organization has recruited outsiders to participate in a financially motivated attack, said Mor Ahuvia, cybercrime communications specialist for RSA FraudAction. The attackers are promising their recruits a cut of the profits, and are requiring an initial investment in hardware and training in how to deploy the Gozi Prinimalka Trojan, Ahuvia added. Also, the gang will only share executable files with their partners, and will not give up the Trojan's compilers, keeping the recruits dependent on the gang for updates

Generally, cybercrime gangs deploy as few as five individual botmasters to help in successful campaigns; with this kind of scale, banks could be facing up 30 times the number of compromised machines and fraudulent transfers, if the campaign is successful.

"This Trojan is not well known. This is not SpyEye or Citadel; it's not available for everyone to buy," Ahuvia said. "Security vendors and antivirus signatures are less likely to catch it or be familiar with it. It will be tricky for vendors to detect and block it. This gang is keeping a tight hold on the compiler. By only giving up executable files, they can control how any antivirus signatures are in the wild and keep unique signatures to a minimum."

As many as 30 banks have been targeted, many of them well known and high profile, Ahuvia said. RSA said the gang is targeting American banks because of past success in beating their defenses, as well as a lack of two-factor authentication required for wire transfers.Some European banks, for example, require consumers to use two-factor authentication. She added that RSA FraudAction was unsure how far along the recruitment campaign had gone, or when the attacks would launch.

"There is the chance that once we've gone public, they may abandon their plans because there's too much buzz around it," Ahuvia said. "On the other hand, I don't think anything we know will have such

a dramatic effect on them. There are so many Trojans available and so many points of failure in security that could go wrong, that they'd still have some chance of success."

RSA's researchers were able to make the connection to the Gozi Prinimalka Trojan, which has been in circulation since 2008 and responsible for $5 million in fraud-related losses. Prinimalka is similar to the Gozi Trojan in technical and operational aspects, RSA said, leading to speculation the HangUp Team, which was tied to previous Gozi attacks, is behind this attack as well. Prinimalka is Russian for the word "receive" and is a folder name in every URL patch given by this particular gang to its crimeware servers.

Prinimalka uses the same bot-to-server communication pattern and URL trigger list as Gozi, RSA said. But deployment of the two Trojans is different: Gozi writes a single DLL file to bots upon deployment, while Prinimalka writes two, an executable file and a DAT file which reports to the command and control server.

Once the Trojan is launched, the botmaster fires up a virtual machine synching module. The module then duplicates the victim's computer, including identifiable features such as time zone, screen resolution, cookies, browser type and version, and software identification, RSA said. This allows the botmaster to impersonate the victim's machine and access their accounts. Access is carried out over a SOCKS proxy connection installed on the victim's machine, RSA said.

The cloned virtual system then can move about on the genuine IP address of the compromised machine when accessing the bank website. Taking it a step further, the attackers deploy VoIP phone flooding software that will prevent the victim from receiving a confirmation call or text alerting them to unusual transfer activity, RSA said.

"They are looking for this to be a quick campaign," Ahuvia said. "They want to make as much as they can until the banks and users harden their systems. They want to cash out quickly."

Commenting on this Article will be automatically closed on January 4, 2013.

EXHIBIT C

No slowdown in sight for cyberattacks

By Byron Acohido, USA TODAY

Updated 7/30/2012 10:30 AM

LAS VEGAS - Cyber attacks are accelerating at a pace that suggests the Internet - already a risky environment - is likely to pose a steadily growing threat to individuals and companies for years to come.

That's the somber consensus of security and Internet experts participating in the giant Black Hat cybersecurity conference that concluded here this week.

Internet-generated attacks comprise "the most significant threat we face as a civilized world, other than a weapon of mass destruction," Shawn Henry, former head of the FBI's cybercrime unit, told some 6,500 attendees in a keynote address.

Getty Images

Internet-generated attacks comprise the most significant threat we face as a civilized world, other than a weapon of mass destruction," according to one security expert.

Joe Stewart, Dell SecureWorks' director of malware research, presented research detailing the activities of two large cyber gangs, one based in Shanghai the other in Beijing, that have cracked into the networks of thousands of companies over the past half dozen years.

The attacks invariably begin by infecting the computer of one employee, then using that machine as a toehold to patiently probe deep into the company's network. The end game: to steal customer lists, patents, bidding proposals and other sensitive documents.

Each gang is made up of dozens of employees playing complementary roles in attacks that are "stealthy and persistent," says Stewart. "Even if they do get discovered and get kicked out of a network, they come back, targeting a different employee."

Another gang, analyzed by Dell SecureWorks' researcher Brett Stone-Gross, has been blasting out spam, designed to slip past spam filters. The messages carry instructions to click on a link to read bogus delivery invoices, airline reservations or cellphone bills. The link, however, takes the user to a web page that installs malicious software.

Stone-Gross said the gang currently has access to 678,000 infected PCs, some of which are used to carry out its lucrative specialty: orchestrating fraudulent wire transfers from online banking accounts.

Meanwhile, a different category of hackers is stepping up attacks, not on individual PCs, but on company websites. Website attacks now routinely occur thousands of times each, as criminals probe for ways to breach databases carrying usernames and passwords and other valuable data, says David Koretz, general manager of website security firm Mykonos, a division of Juniper Networks.

Some successful website hackers enjoy boasting —by publically posting some, if not most, of the stolen data. That's happened recently with data stolen from online retailer Zappos, matchmaking site eHarmony, business social networking site LinkedIn and search giant Yahoo, Koretz says.

Experts say web attacks continue to escalate partly because powerful, easy-to-use hacking programs are widely available for free. What's more, opportunities for an intruder to take control of an individual's PC, or access and probe a company's network, are multiplying as society uses more Internet-delivered services and Internet-connected mobile devices.

"It's easier and safer for a criminal to steal money from an online bank account, rather than have to walk into a bank — or to steal intellectual property in an online setting, rather than have to send in a human spy," says Eddie Schwartz, chief security officer of security firm RSA, a division of EMC.

Posted 7/27/2012 10:34 AM | Updated 7/30/2012 10:00 AM

EXHIBIT D

Threat Level
Privacy, Crime and Security Online
Hacks and Cracks
Cybersecurity

Hackers Release 1 Million Apple Device IDs Allegedly Stolen From FBI Laptop

By Kim ZetterEmail Author
09.04.12
12:49 PM

Photo: Wired

The hacker group AntiSec has released 1 million Apple device IDs that they say they obtained from an FBI computer they hacked.

The hackers say they actually stole 12 million IDs, including personal information, from the hacked FBI computer, but released only 1 million in an encrypted file published on torrent sites.

In a lengthy post online, the hackers wrote that last March, they hacked a laptop belonging to an FBI agent named Christopher K. Stangl from the bureau's Regional Cyber Action Team and the New York FBI office's Evidence Response Team.

The hackers say the IDs were stored in a file on Stangl's desktop titled "NCFTA_iOS_devices_intel.csv."

The file, according to the hackers, contained a list of more than 12 million Apple iOS devices, including Unique Device Identifiers (UDID), user names, names of devices, types of devices, Apple Push Notification Service tokens, ZIP codes, cellphone numbers, and addresses. The hackers released only 1 million UDIDs, however, and did not release the accompanying personal information for the IDs.

Apple UDIDs are a 40-character alphanumeric string that is unique to each Apple device.

It's not known why the FBI possessed the Apple IDs. The hackers suggested in a tweet from the the @AnonymousIRC account, that the FBI was using the information to track users.

Stangl may have been targeted because he was on an e-mail that members of Anonymous intercepted last January. The e-mail was sent to several dozen U.S. and European law-enforcement personnel to participate in a conference call discussing efforts to investigate Anonymous and other hacking groups. The email included a call-in number for the discussion, which members of Anonymous recorded and posted online last February.

The hackers say they released the Apple UDIDs so that people would know that the FBI may be tracking their devices and also because, they wrote in their online post, "we think it's the right moment to release this knowing that Apple is looking for alternatives for those UDID currently ... but well, in this case it's too late for those concerned owners on the list."

Apple has been criticized for hard-coding the ID's in devices, since they can be misused by application developers and others to identify a user, when combined with other information, and track them. Last April, Apple began rejecting applications that track UDIDs.

The Next Web has created a tool for users to check if their Apple UDID is among those that the hackers released.

Related

You Might Like

Related Links by Contextly

EXHIBIT E

Cyber defenders urged to go on the offense

By Glenn Chapman (AFP) – Jul 26, 2012

LAS VEGAS — Computer security champions on Wednesday were urged to hunt down and eliminate hackers, spies, terrorists and other online evildoers to prevent devastating Internet Age attacks.

The first day of briefings at a prestigious Black Hat computer security gathering here opened with a former FBI cyber crime unit chief calling for a shift from defense to offense when it comes to protecting networks.

"We need warriors to fight our enemies, particularly in the cyber world right now," Shawn Henry said in a Black Hat keynote presentation that kicked off with dramatic video of hostage rescue teams training.

"I believe the threat from computer network attack is the most significant threat we face as a civilized world, other than a weapon of mass destruction."

The peril grows as water supplies, power grids, financial transactions, and more rely on the Internet and as modern lives increasingly involve working and playing on smartphones or tablet computers, according to Henry.

He rolled off a list of adversaries ranging from spies and well-funded criminals to disgruntled employees with inside knowledge of company networks.

"Cyber is the great equalizer," Henry said.

"With a $500 laptop with an Internet connection anybody, anywhere in the world can attack any organization, any company," he continued. "The last time I checked, that was about 2.3 billion people."

After 24 years of working for the FBI, Henry in April switched to the private sector as the head of a division at startup CrowdStrike specializing in cyber attack incident responses and identifying adversaries.

The computer security industry to expand its arsenal beyond just building walls, filters and other safeguards against online intruders to include watching for, and gathering intelligence on, culprits who have slipped through.

"It is not enough to watch the perimeter," Henry said, equating computer security to protecting real world offices. "We have to be constantly hunting; looking for tripwires."

In the cyber world, that translates into monitoring system activities such as whether files have been accessed or changed and by whom.

"The sophisticated adversary will get over that firewall and walk around, like an invisible man," Henry said. "We have to mitigate that threat."

Tactics for fighting cyber intruders should include gathering information about how they operate and the tools used, and then sharing the data in the industry and with law enforcement agencies in relevant countries.

"Intelligence is the key to all of this," Henry said. "If we understand who the adversary is, we can take specific actions."

Teamwork between governments and private companies means that options for responding to identified cyber attackers can range from improved network software to political sanctions or even military strikes, according to Henry.

"You can't make every school, every mall, every university, and every workplace impenetrable," Henry said. "We have to look at who the adversary is and stop them in advance of them walking in."

Black Hat founder Jeff Moss, the self-described hacker behind the notorious Def Con gathering that starts here on Thursday, backed Henry's argument.

"Maybe we need some white blood cells out there; companies willing to push the edge and focus on threat actors," Moss said, calling on the computer security community to "raise the immunity level."

Moss is head of security at the Internet Corporation for Assigned Names and Numbers, which oversees the world's website addresses.

"So, am I Luke, or am I Darth Vader; sometimes I'm not sure," Moss quipped about his roles in the hacker realm and the computer security industry.

"It depends upon which day and who asks."

Moss proposed that cyber attackers also be fought on legal fronts, with companies taking suspected culprits to court.

"I can't print money; I can't raise an army, but I can hire lawyers and they are almost as good," Moss said. "One way to fight the enemy is you just sue them."

Henry feared that it may take an Internet version of the infamous 9/11 attack in New York City to get the world to take the cyber threat to heart.

"We need to get down range and take them out of the fight," Henry said.

Former FBI cyber crime unit chief Shawn Henry was the keynote speaker at the Black Hat computer security gathering (AFP/Getty Images/File)

Map

"As well-trained, well-equipped cyber warriors you can have an impact; the stakes are high."

More »

EXHIBIT CC

Michael Dugas

3rd

Associate Attorney at Prenda Law Inc.

Minneapolis, Minnesota | Law Practice

Education University of Minnesota-Twin Cities

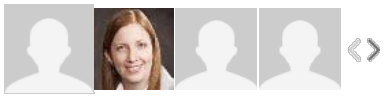
Connect | Send InMail

28 connections

Full profiles for 3rd-degree connections are available only to premium account holders.

Upgrade your account »

PEOPLE SIMILAR TO MICHAEL



Reynaldo Quinones
Attorney at Riguer Silva, LLC
Connect

PEOPLE ALSO VIEWED

Paul Hansmeier
Partner at Alpha Law Firm LLC

Show Wang
Law Student

Padraigin Browne
Associate Attorney at Shumaker & Sieffert

Luqman Lawal
Graduate consultant

Heiko Carstens
Senior Manager Consulting FS bei KPMG

John Steele
Of Counsel to Various Intellectual Property Firms

Alexis Orenstein
Corporate Associate at Simpson Thacher & Bartlett LLP

Xiyan Zhang
Attorney, P.E.

Rory Wellever
Associate at Kirkland & Ellis LLP

Reynaldo Quinones
Attorney at Riguer Silva, LLC

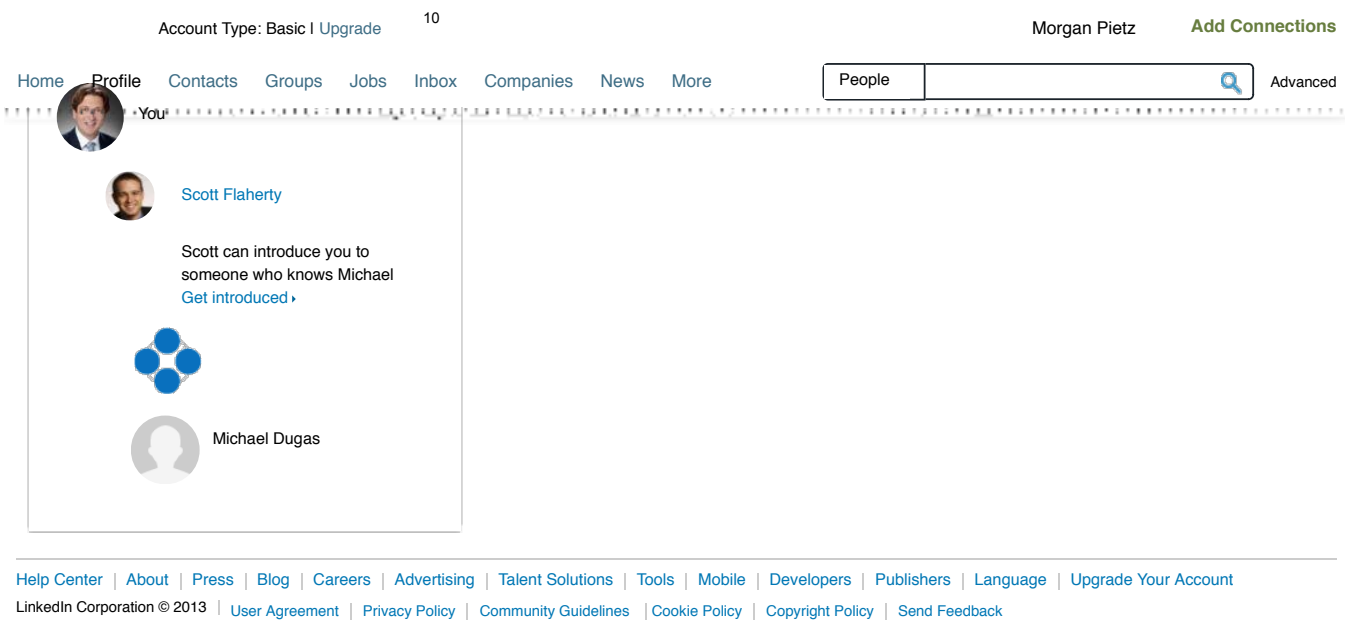


EXHIBIT DD

NOT FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

FILED

OCT 24 2012

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

In re: ESTATE OF FERDINAND E. MARCOS HUMAN RIGHTS LITIGATION,	No. 11-15487 D.C. No. 1:03-cv-11111-MLR
CELSA HILAO; ADORA FAYE DE VERA, Plaintiffs - Appellees, v. THE ESTATE OF FERDINAND E. MARCOS, Defendant - Appellant.	MEMORANDUM*

Appeal from the United States District Court
for the District of Hawaii
Manuel L. Real, District Judge, Presiding

Argued and Submitted October 15, 2012
Honolulu, Hawaii

* This disposition is not appropriate for publication and is not precedent except as provided by 9th Cir. R. 36-3.

Before: REINHARDT, THOMAS, and PAEZ, Circuit Judges.

The Estate of Ferdinand E. Marcos (hereinafter "Marcos") appeals a $353,600,000 contempt judgment awarded to a class of human rights victims (hereinafter "Hilao"). Marcos argues on appeal that, because the underlying damages judgment expired in 2005[1] and because the $100,000 per day contempt sanction upon which the contempt judgment was based was coercive in nature,[2] the contempt judgment is unenforceable. We review findings of civil contempt and the amount of a civil contempt sanction for abuse of discretion. *FTC v. Affordable Media, LLC*, 179 F.3d 1228, 1229 (9th Cir. 1999). Underlying factual findings are reviewed for clear error. *Id.* We have jurisdiction under 28 U.S.C. § 1291, and we affirm.

Marcos's argument is likely waived. The argument that Marcos made in the district court was that the contempt judgment was unenforceable under state law, because it had expired under Haw. Rev. Stat. § 657-5. The district court rejected this argument, and Marcos did not appeal that determination, although it did appeal

[1] The underlying damages judgment in an action against Marcos by Hilao expired in 2005 pursuant to Hawaii's ten-year statute of limitations for civil judgments. Haw. Rev. Stat. § 657-5.

[2] The contempt judgment was issued in 2011, and it covered the failure of Marcos to pay the court's contempt sanction from 1995 to 2005.

the decision. Marcos now argues on appeal that the contempt judgment is unenforceable under federal law, because coercive sanctions are unenforceable when the underlying damages judgment has expired. This is a new argument, and we "do[] not consider an issue not passed upon below." *Dodd v. Hood River Cnty.*, 59 F.3d 852, 863 (9th Cir. 1995) (internal quotation and citation omitted). Marcos contends that it "obliquely" made this argument in its December 2010 status report statement. We agree that this reference was oblique; it was, in fact, a single sentence of a single paragraph of a five-page memorandum to the district court. Moreover, the paragraph lacked legal citation and began with "Put another way," suggesting that Marcos was simply restating the state law argument in different terms. Thus, Marcos did not raise this argument "sufficiently for the trial court to rule on it." *Whittaker Corp. v. Execuair Corp.*, 953 F.2d 510, 515 (9th Cir. 1992) (quoting *In re E.R. Fegert, Inc.*, 887 F.2d 955, 957 (9th Cir. 1989)).

Independent of waiver, we reject Marcos' argument on the merits. Even if Marcos is correct that the contempt sanction was coercive, it was also clearly compensatory.[3] The district court ordered that the $100,000 per day sanction be paid to the plaintiff, Hilao, not the court. *See Falstaff Brewing Corp. v. Miller*

[3] Marcos has conceded that a compensatory contempt judgment is enforceable even when the underlying damages judgment has expired.

Brewing Co., 702 F.2d 770, 779-80 (9th Cir. 1983). Additionally, the district court explained that the $100,000 per day amount was "necessary and appropriate" because Marcos's contumacious conduct was causing direct harm to Hilao, including $55,000 per day from lost interest and additional losses due to Marcos's dilatory tactics. Because a contempt sanction can be *both* coercive and compensatory, *U.S. v. United Mine Workers of America*, 330 U.S. 258, 303-04 (1947); *Union of Prof. Airmen v. Alaska Aeronautical Ind., Inc.*, 625 F.2d 881, 883 (9th Cir. 1979), and because no party has asked the court to allocate the $100,000 per day amount between compensatory and coercive components, the district court did not abuse its discretion in treating the entirety of the $100,000 per day sanction as compensatory.

In view of the above, we hold that the $353,600,000 contempt judgment is properly enforceable by Hilao.

AFFIRMED.