Hawaii High School Mock Trial Competition

The 2017 Mock Trial
Criminal Case

IN THE CIRCUIT COURT
OF THE SEVENTH CIRCUIT
STATE OF HAWAII

State of Hawaii,	)	
	)	**Case No.**
Prosecution,	)	**2015-GS-47-0926**
	)	
v.	)	**Case No.**
	)	**2015-GS-47-0927**
Ele Woods,	)	
	)	**Case No.**
Defendant.	)	**2015-GS-47-0928**
	)	

NOTE: All characters, names, events, places, and circumstances in this Mock Trial case are fictitious.

A PROJECT OF THE YOUNG LAWYERS DIVISION

OF THE HAWAII STATE BAR ASSOCIATION

The 2017 Hawaii High School Mock Trial case was adapted and revised by the Mock Trial Committee from the 2015 South Carolina trial case, State of South Carolina v. Peyton Scott, written by Donald N. Lanier.

January 2017

2017
MOCK TRIAL
CASE
(High School)

January 2017

2017 High School Mock Trial Case:

Case Overview

Throughout the modern era, there has been an ongoing struggle between tax-paying, law-abiding citizens, and those who seek to steal from them. In the 1950s and 60s this was done through the use of check forgeries. In the 1980s, theft and fraud began to move to electronic means with credit cards. In the late 1990's, theft transitioned to the internet with America Online and various other Internet Service Providers (ISP). In the current decade with the exponential increase of online shopping, the theft and fraud has moved into the arena of electronic hacking. Whereas previous methods of fraud targeted people individually, hackers are now able to defraud thousands if not millions of people in a single attack.

In the fall of 2015, Ele Woods and Micah Ross were juniors at West Waiakea University (WWU). Both were computer engineering majors. During the course of the semester, Ele Woods was working with Professor Hayden Litt in an effort to evaluate the security risks of Lilikoi's, a Hawaii based retailer.

During the research conducted by Professor Hayden Litt, the online shopping site of Lilikoi's was hacked in excess of the contract terms. During the hack, customer information including credit card numbers and expiration dates were exposed. Following this data exposure, 35 Hawaii residents became victims of fraud, and more than $10,000 in fraudulent purchases were made. Through the Director of Operations of Lilikoi's, the State Law Enforcement Division (SLED) Computer Crimes Division was able to trace back the source of the hack to a MAC address of a computer on the WWU campus.

Following a search and seizure warrant executed by SLED at the on campus apartment of Ele Woods and Micah Ross, Ele Woods was charged with financial transaction card fraud, financial transaction card or number theft, and computer crime. Micah Ross worked with SLED and alleged that everything seized within the apartment was the property of Ele Woods. Ele Woods admitted to causing the breach, but claimed to charge only $10 on each of the five contracted credit cards. Further, Ele Woods reported the website breach to Professor Litt as part of the contract with WWU and Lilikoi's.

****

The introduction is background material for informational purposes only.
It is not to be considered part of the case materials.

****

PLEADINGS

WITNESSES

Casey Specter

ARREST WARRANT NUMBER

DIRECT INDICTMENT

ACTION OF GRAND JURY

TRUE BILL

Brynn Forsyth

Foreperson of Grand Jury

Date: November 4, 2015

VERDICT

Brynn Forsyth

Foreperson of Grand Jury

Date: November 4, 2015

DOCKET NO. 2015-GS-47-0926

The State of Hawaii County of Kaimana

THE STATE OF HAWAII

vs.

ELE WOODS

INDICTMENT FOR

H.R.S.: § 16-14-60

STATE OF HAWAII	)	INDICTMENT
	)	
COUNTY OF Kaimana	)	

At a Court of General Sessions, convened on November 4, 2015, the Grand Jurors of Kaimana County present upon their oath:

FINANCIAL TRANSACTION CARD FRAUD HAWAII REVISED STATUTES. § 16-14-60

That Ele Woods did, in Kaimana County, on or about September 2015, commit the crime of Financial Transaction Card Fraud in that the Defendant, Ele Woods, did willfully, knowingly, maliciously, and without authorization or for an unauthorized purpose accessed Lilikoi's credit card data for the purpose of obtaining property greater than $10,000, contrary to the laws of the State of Hawaii, in the West Waiakea University, at Apartment 230 South Quad, Kaimana County, Hawaii.

Against the peace and dignity of the State, and contrary to the statute in such case made and provided.

David W. Miller

DAVID W. MILLER, SOLICITOR

WITNESSES

Casey Specter

ARREST WARRANT NUMBER

DIRECT INDICTMENT

ACTION OF GRAND JURY

TRUE BILL

Brynn Forsyth

Foreperson of Grand Jury

Date: November 4, 2015

VERDICT

Brynn Forsyth

Foreperson of Grand Jury

Date: November 4, 2015

DOCKET NO. 2015-GS-47-0927

The State of Hawaii County of Kaimana

THE STATE OF HAWAII

vs.

ELE WOODS

INDICTMENT FOR

H.R.S.: § 16-14-20

STATE OF HAWAII	)	INDICTMENT
	)	
COUNTY OF Kaimana	)	

At a Court of General Sessions, convened on November 4, 2015, the Grand Jurors of Kaimana County present upon their oath:

FINANCIAL TRANSACTION CARD OR NUMBER THEFT HAWAII REVISED STATUTES. § 16-14-20

That Ele Woods did, in Kaimana County, on or about September 2015, commit the crime of Financial Transaction Card or Number Theft in that the Defendant, Ele Woods, unlawfully obtained the financial transaction card or number of at least 35 Hawaii individuals, to wit, credit card numbers, without authorization or permission, contrary to the laws of the State of Hawaii, in the West Waiakea University, at Apartment 230 South Quad, Kaimana County, Hawaii.

Against the peace and dignity of the State, and contrary to the statute in such case made and provided.

David W. Miller

DAVID W. MILLER, SOLICITOR

WITNESSES

Casey Specter

ARREST WARRANT NUMBER

DIRECT INDICTMENT

ACTION OF GRAND JURY

TRUE BILL

Brynn Forsyth

Foreperson of Grand Jury

Date: November 4, 2015

VERDICT

Brynn Forsyth

Foreperson of Grand Jury

Date: November 4, 2015

DOCKET NO. 2015-GS-47-0928

The State of Hawaii County of Kaimana

THE STATE OF HAWAII

vs.

ELE WOODS

INDICTMENT FOR

H.R.S.: § 16-16-20

STATE OF HAWAII	)	INDICTMENT
	)	
COUNTY OF Kaimana	)	

At a Court of General Sessions, convened on November 4, 2015, the Grand Jurors of Kaimana County present upon their oath:

COMPUTER CRIME HAWAII REVISED STATUTES. § 16-16-20

That Ele Woods did, in Kaimana County, on or about September 2015, willfully, knowingly, maliciously, and without authorization, accessed the computer system of Lilikoi's for the purpose of obtaining money or property with the intent to defraud, and that the loss to Lilikoi's exceeded $10,000, contrary to the laws of the State of Hawaii, in the West Waiakea University, at Apartment 230 South Quad, Kaimana County, Hawaii.

Against the peace and dignity of the State, and contrary to the statute in such case made and provided.

David W. Miller

DAVID W. MILLER, SOLICITOR

	)	SEVENTH JUDICIAL CIRCUIT
	)	
STATE OF HAWAII,	)	COURT OF GENERAL SESSIONS
	)	
Prosecution,	)	
vs.	)	2015-GS-47-0926
	)	2015-GS-47-0927
ELE WOODS,	)	2015-GS-47-0928
	)	
Defendant.	)	
	)	
	)	
	)	**DEMAND FOR JURY TRIAL**
	)	

The State of Hawaii filed three Indictments against Defendant Ele Woods. The Indictments were true billed by the Grand Jury on November 4, 2015. Defendant pled not guilty to all charges.

I, the undersigned, do hereby demand a jury trial in the above matter.

Dated: November 4, 2015

Signed: Ele Woods
Ele Woods, Defendant

	)	SEVENTH JUDICIAL CIRCUIT
	)	
STATE OF HAWAII,	)	COURT OF GENERAL SESSIONS
	)	
Prosecution,	)	
vs.	)	2015-GS-47-0926
	)	2015-GS-47-0927
ELE WOODS,	)	2015-GS-47-0928
	)	
Defendant.	)	
	)	
	)	
	)	
	)	

Pre-Trial Order

On this the 7th day of January 2016, the above-captioned matter came before the undersigned judge for pretrial conference. The parties, appearing through their counsel, indicated their agreement to, and approval of, the terms of this Order, and requested that it be made the Order of this Court. The terms of this order, accordingly, shall not be altered, except upon a showing of good cause.

I. Statement of Case

The State of Hawaii charged the Defendant, Ele Woods, with Financial Transaction Card Fraud, Financial Transaction Card Fraud or Number Theft, and Computer Crime, to wit; Ele Woods did unlawfully gain access to the secure financial servers of Lilikoi's, further unlawfully removed 4,000 credit card numbers with expiration dates, and later used 35 of those credit cards to unlawfully purchase various items from Lilikoi's in excess of $10,000, contrary to the laws of the State of Hawaii, and the good order, peace and dignity thereof. Upon arraignment, Ele Woods pled not guilty to all charges.

II. Stipulations of the Parties

The parties have entered into the following stipulations, which shall not be contradicted or challenged:

1. All exhibits included in the case materials are authentic and are accurate copies of the originals. No objections to the authenticity of the exhibits will be entertained. The only exhibits to be used at trial are those included in the case materials provided.

2. No witness may be examined or cross-examined as to the contents of anything not included in the case materials. This includes, but is not limited to, information found on the internet, social media, books, magazines, or other publications.

3. The chain of custody for evidence is not in dispute.

4. Though evidence of a crime, the records of credit card numbers and expiration dates from the security breach are considered confidential victim information and are not open for inspection in court records.

5. The signatures on the witness statements and all other documents are authentic.

6. All students at West Waiakea University are required to have a computer commonly referred to as a “laptop.”

7. Class attendance records from West Waiakea University are not available.

8. James Myrick has retired to Aruba, and is unavailable to testify.

9. Neither Officer TJ McCabe, nor Sgt. Harrelson have any substantive information to offer the case and therefore are not to be called.

10. All witnesses who were questioned by law enforcement were properly advised of their Miranda rights. The search of the on campus apartment was conducted with a properly signed and executed warrant, and therefore was proper and in accordance with the law.

11. The required signature confirmation on the USPS shipping receipt is unrecognizable and therefore is not offered as an exhibit.

12. No hats of any color or kind may be worn in court.

13. The charge of the Court is accurate in all respects, and no objections to the charge will be entertained.

14. Exhibits 1, 2, 3, 4, 5, 6, 7, and 11 are kept in the ordinary course of business or as part of the ordinary conduct of an organization or enterprise where it was part of the ordinary business of that organization, business or enterprise, to compile the data or information. The information was made for the purpose of recording the occurrence of an event, act, condition, opinion, or diagnosis that takes place in the ordinary course of the business or enterprise; entry in the record or the compiling of the data was made at or near the time when the event took place; and the recording of the event was made by someone who has personal knowledge of the records in question. The custodian of record is not necessary to offer it, but anyone with knowledge may do so.

15. All parties are responsible for knowing the technical terms of the information technology industry located in the stipulations (“Terminology” section), in the statutes, and in the jury instructions clarified for the purposes of this case.

16. All witnesses have been advised of and have waived their 5th Amendment right against self-incrimination.

17. The use of a calendar to verify days of the week is acceptable, but may not be offered as an exhibit.

TERMINOLOGY

Algorithms: A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

ASCII Characters: Special keyboard characters involving use of a shift or control key to create characters, such as @#$%*&).

Biometrics: Distinctive, measurable characteristics used to identify a person for security purposes. May include, but is not limited to fingerprints, face recognition, DNA, palm print, iris recognition, and retina recognition.

Black Hat: A slang term for a hacker who violates computer security for little reason beyond maliciousness or for personal gain.

Brute Force Attack: A type of computer attack against encrypted data which systematically exhausts all possible login passwords, for example programming a computer to use all known words in the English language along with all possible two digit number combinations with those words. These searches are time consuming and if successful, allows access to the computer system. This form of attack does not search for vulnerabilities in the computer code controlling the machine.

Content Mgmt. System (CMS): A computer program designed to allow people to publish, edit, and modify content on a website or a series of websites.

C V V Number: Card Verification Value is on the back of a credit card or debit card, which is a three digit number on VISA®, MasterCard® and Discover® cards.

Fail Safe: A type of additional security provision in which after logging onto the computer, one must complete an action or a series of actions to prevent a lockout and reformat of the hard drive.

Forging: To produce a copy or imitation of a document, signature, banknote, or work of art for the purpose of deception. *(See also MAC Address Forging.)*

Hacking: The act of seeking out and exploiting weakness in a computer system or network system.

Internet Protocol (IP): The system of sending data packets over the internet, which has been the standard from the late 1970's to present for data transmission. Also referred to as TCP/IP.

IP Address: A unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

IP Address Spoofing: The creation of Internet Protocol (IP) packets with a source IP address for the purpose of concealing the identity of the sender or for impersonating another computer system.

Media Access Control address (MAC address): A unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most network technologies.

MAC Address Forging: Masking and then substituting the MAC address of a computer while on a physical network in order to impersonate another operator on the same system.

Non-Disclosure Agreement (NDA): Also called a confidentiality agreement, the NDA prevents a person working for a business to reveal information about that business to outside persons under penalty of civil litigation and financial burden.

Ordering Tools (scan gun): A type of tool common to the retail industry with a handle resembling that of a gun. The purpose of this device is to scan the barcode of an item to order more.

Point of Sale (POS) Devices: A computer or tablet system which serves as a general check out device for making sales in a retail business; may also contain inventory and employee information access.

Secure Transaction Server: A server that works with encrypted data.

Server: A computer running a type of software, which makes it capable of accepting requests from other computers and giving responses accordingly.

Spoofing: To trick, or fool a person or electronic device. *(See also IP Address Spoofing.)*

Virtual Presence: A common term referencing the internet business presence of a traditional physical store.

White Hat: A slang term for an ethical hacker, or someone who serves as a computer security expert in the field of testing and vulnerability strengthening.

WiFi: A local area wireless technology that allows an electronic device to exchange data or connect to the internet.

WiFi Sniffer: A tool specifically designed to detect wireless networks and security encryption or lack of same.

Wireless Router: A device that performs the functions of a traditional router, but also includes the functions of a wireless access point; commonly used to allow an electronic device to exchange data or connect to the internet.

IT IS SO ORDERED, this day of this round of the High School Mock Trial competition.

/s/ Presiding Judge

The Honorable Presiding Judge

HAWAII CRIMINAL LAW STATUTES

[Revised for purposes of Mock Trial.]

Hawaii Revised Statutes. § 16-14-10. Definitions - Financial Transaction Card Crime Act.

…

(2) "Cardholder" means the person or organization to whom or for whose benefit the financial transaction card is issued by an issuer.

…

(4) "Financial transaction card" means any instrument or device whether known as a credit card, credit plate, bank services card, banking card, check guarantee card, debit card, or by any other name, issued with or without fee by an issuer for the use of the cardholder in obtaining money, goods, services, or anything else of value on credit.

(5) "Issuer" means the business organization or financial institution or its duly authorized agent which issues a financial transaction card.

(6) "Personal identification code" means a numeric or alphabetical code assigned to the cardholder of a financial transaction card by the issuer to permit authorized electronic use of that financial transaction card.

(7) "Presenting" means those actions taken by a cardholder or any person to introduce a financial transaction card into an automated banking device, including utilization of a personal identification code, or merely displaying or showing a financial transaction card to the issuer, or to any person or organization providing money, goods, services, or anything else of value, or any other entity with intent to defraud.

(8) "Receives" or "receiving" means acquiring possession or control of a financial transaction card or accepting a financial transaction card as security for a loan.

Hawaii Revised Statutes. § 16-14-60. Financial Transaction Card Fraud.

A person is guilty of Financial Transaction Card Fraud when, with intent to defraud the issuer, a person or organization providing money, goods, services, or anything else of value, or any other person, he:

(1) Uses a financial transaction card obtained or retained, or which was received with knowledge that it was obtained or retained, in violation of Section § 16-14-20, and

(2) Obtains money, goods, services, or anything else of value by:
   (a) Representing without the consent of the specified cardholder that he has permission to use it; or
   (b) Presenting the financial transaction card without the authorization or permission of the cardholder; or
   (c) Representing that he is the holder of a card and the card has not in fact been issued.

A person who violates the provisions of this subsection is guilty of a misdemeanor and, upon conviction, must be fined not more than $1,000 or imprisoned not more than one year, or both, if the value of all money, goods, services, and other things of value furnished in violation of this section does not exceed $500 in any six-month period. If the value exceeds $500 in a six-month period, a person is guilty of a felony and, upon conviction, must be fined not less than $3,000 or more than $10,000, or imprisoned not more than ten years, or both.

Hawaii Revised Statutes. § 16-14-20. Financial Transaction Card or Number Theft.

A person is guilty of Financial Transaction Card or Number Theft when he:

(1) Takes, obtains, or withholds a financial transaction card or number from the person, possession, custody, or control of another without the cardholder's consent and with the intent to use it; or who, with knowledge that it has been so taken, obtained, or withheld, receives the financial transaction card or number with intent to use it, sell it, or transfer it to a person other than the issuer or the cardholder; or

(2) Receives a financial transaction card or number that he knows to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder, and who retains possession with intent to use it, sell it, or transfer it to a person other than the issuer or the cardholder; or

(3) Is not the issuer, and sells a financial transaction card or number or buys a financial transaction card or number from a person other than the issuer.

A person who commits Financial Transaction Card or Number Theft must be punished as follows:

(1) If the number of financial transaction cards and numbers is less than five, the person is guilty of a misdemeanor and must be imprisoned not more than 30 days, or fined more than $1,000 or both.

(2) If the number of financial transaction cards and numbers is 5 - 100, the person is guilty of a felony and must be imprisoned not more than 3 years, or fined more than $5,000, or both.

(3) If the number of financial transaction cards and numbers in excess of 100, the person is guilty of a felony and must be imprisoned not more than 5 years, or fined more than $10,000 or both.

Hawaii Revised Statutes. § 16-16-20. Computer Crime Offenses; Penalties.

(1) It is unlawful for a person to willfully, knowingly, maliciously, and without authorization or for an unauthorized purpose to:

  (a) Directly or indirectly access or cause to be accessed a computer, computer system, or computer network for the purpose of:

    (i) Devising or executing a scheme or artifice to defraud;

    (ii) Obtaining money, property, or services by means of false or fraudulent pretenses, representations, promises; or

    (iii) Committing any other crime.

  (b) Alter, damage, destroy, or modify a computer, computer system, computer network, computer software, computer program, or data contained in that computer, computer system, computer program, or computer network or introduce a computer contaminant into that computer, computer system, computer program, or computer network.

(2) A person is guilty of computer crime in the first degree if the amount of gain directly or indirectly derived from the offense exceeds $10,000. Computer crime in the first degree is a felony and, upon conviction, a person must be fined not more than $50,000 or imprisoned not more than five years, or both. A person is guilty of computer crime in the second degree if the amount of gain directly or indirectly derived from the offense is not more than $10,000 Computer crime in the second degree is a felony and, upon conviction, a person must be fined not more than $10,000 or imprisoned not more than three years, or both.

	)	SEVENTH JUDICIAL CIRCUIT
	)	
STATE OF HAWAII,	)	COURT OF GENERAL SESSIONS
	)	
Prosecution,	)	
vs.	)	2015-GS-47-0926
	)	2015-GS-47-0927
ELE WOODS,	)	2015-GS-47-0928
	)	
Defendant.	)	
	)	
	)	
	)	
	)	

Jury Instructions

(Note: Jury instructions are <u>NOT</u> to be read to the jury on the day of the Mock Trial competition.)

The Court hereby approves the following jury instructions in the above-captioned case. It notes that the presentation of evidence at trial may warrant additional instructions, and it will consider those instructions at a later date.

(A) Opening Instruction:

You have been selected and sworn as the jury to try this case of the State of Hawaii against Ele Woods. The Defendant is charged with the following offenses: Financial Transaction Card Fraud in violation of Hawaii Revised Statutes § 16- 14-60, Financial Transaction Card or Number Theft in violation of Hawaii Revised Statutes § 16-14-20, and Computer Crime, in violation of the Hawaii Revised Statutes § 16-16-20. The Indictments in this case are the formal method of accusing the Defendant of the crimes. The Indictments are not evidence and you should not allow yourselves to be influenced against the Defendant by reason of the filing of the Indictments. The Defendant has pled not guilty. A plea of not guilty puts at issue each element of the crime with which the Defendant is charged. A plea of not guilty requires the State to prove each element of the crime beyond a reasonable doubt. The Defendant is presumed innocent of the crime and this presumption continues unless and until, after consideration of all the evidence, you are convinced of the Defendant's guilt beyond a reasonable doubt. The Defendant must be found not guilty unless the State produces evidence which convinces you beyond a reasonable doubt of the existence of each element of the crimes. It is your responsibility as jurors to determine the facts from the evidence, to follow the law as stated in the instructions from the presiding judge, and to reach a verdict of not guilty or guilty based upon the evidence.

We will now have opening statements of the counsel. Statements and arguments of counsel are not evidence. The purpose of opening statements and closing arguments is to assist you, the jury, in making a decision in this case; however, that decision must be based upon the evidence in this case, which consists of the testimony delivered under

oath in this trial, any documents or other items introduced into evidence during this trial, and the stipulations of the parties.

(B) Closing Instructions:

(1) Introduction:

Now that all the evidence has been presented, it is my duty under the law to give you the instructions that apply in this case. The instructions contain all rules of the law that are to be applied by you, and all the rules by which you are to weigh the evidence and determine the facts at issue in deciding this case and reaching a verdict. You must consider the instructions as a whole. All the testimony and evidence that is proper for you to consider has been introduced in this case. You should not consider any matter of fact or of law except that which has been given to you during the trial of this case.

It is your responsibility as jurors to determine the facts from the evidence, to follow the rules of law as stated in these instructions, and to reach a fair and impartial verdict of guilty or not guilty based upon the evidence, as you have sworn you would do. You must not use any method of chance in arriving at a verdict, but must base your verdict on the judgment of each juror.

(2) Elements of the Charges:

In this matter, the Defendant has been charged with three crimes:

(a) Financial Transaction Card Fraud, under Hawaii Revised Statutes. § 16-14-60;
(b) Financial Transaction Card or Number Theft, under Hawaii Revised Statutes. § 16-14-20; and
(c) Violation of the Computer Crime Act, under Hawaii Revised Statutes. § 16-16-20.

To these charges, the Defendant has entered a plea of not guilty. Each charge should be considered separately.

I will now define the elements for each charge:

Financial Transaction Card Fraud – Hawaii Revised Statutes. § 16-14-60:

Under Hawaii Revised Statutes § 16-14-60, and relevant to the Indictment and allegations in this case, a person is guilty of Financial Transaction Card Fraud when he or she, with the intent to defraud the issuer, a person or organization providing money, goods, services, or anything else of value, or any other person, he or she uses a financial transaction card obtained or retained, or which was received with knowledge that it was obtained or retained, in violation of Section § 16-14-20, and obtains money, goods, services, or anything else of value by representing, without the consent of the specified cardholder that he or she has permission to use it; or by presenting the financial transaction card without the authorization or permission of the cardholder; or by representing that he or she is the holder of a card and the card has not in fact been issued.

In this case, the State has alleged that the fraud involves using one or more financial transaction cards without authorization to obtain merchandise from Lilikoi's. Therefore, in order to prove Mr./Ms. Woods guilty of Financial Transaction Card Fraud, the State must prove the following:

(1) The Defendant used one or more financial transaction cards obtained in violation of Section § 16-14-20 by either:
    (a) Representing, without the consent of the specified cardholder that he or she has permission to use it; or by
    (b) Presenting the financial transaction card without the authorization or permission of the cardholder; and that
(2) The use of such card or cards was with the intent to defraud another of money, goods, services, or anything else of value; and that
(3) Money, goods, services, or anything else of value was obtained.

If you find Mr./Ms. Woods guilty of Financial Transaction Card Fraud, you will be asked on the verdict form to determine the amount of "money, goods, services, or anything else of value" which the Defendant obtained in violation of this statute.

Financial Transaction Card or Number Theft – Hawaii Revised Statutes. § 16-14-20:
Under Hawaii Revised Statutes § 16-14-20, and relevant to the Indictment and allegations in this case, a person is guilty of Financial Transaction Card or Number Theft when he or she:

Takes, obtains, or withholds a financial transaction card, or a financial transaction card number, from the person, possession, custody, or control of another, without the cardholder's consent, and with the intent to use it; or who, with knowledge that it has been so taken, obtained, or withheld, receives the financial transaction card or number with intent to use it, sell it, or transfer it to a person other than the issuer or the cardholder.

In this case, the State has alleged that the theft involved financial transaction card numbers obtained from the secure financial servers of Lilikoi's. Therefore, in order to prove Mr./Ms. Woods guilty of Financial Transaction Card or Number Theft, the State must prove the following:

(1) The Defendant took or obtained one or more financial transaction card numbers, from the possession, custody, or control of another; and that
(2) The number or numbers were taken or obtained without the consent of the cardholder(s) to which it or they belonged; and that
(3) The Defendant took or obtained the card number or numbers with the intent to use the card number or numbers.

If you find Mr./Ms. Woods guilty of Financial Transaction Card or Number Theft, you will be asked on the verdict form to determine the number of financial transaction card numbers which the Defendant took or obtained in violation of this statute.

Definitions for Financial Transaction Card Fraud and Financial Transaction Card or Number Theft:
For purposes of deciding whether the State has proven the elements of Financial Transaction Card Fraud and Financial Transaction Card or Number Theft, the following definitions, are provided by our Statutes:

"Cardholder" means the person or organization to whom or for whose benefit the financial transaction card is issued by an issuer.

"Financial transaction card" means any instrument or device whether known as a credit card, credit plate, bank services card, banking card, check guarantee card, debit card, or by any other name, issued with or without fee by an issuer for the use of the cardholder in obtaining money, goods, services, or anything else of value on credit.

"Issuer" means the business organization or financial institution or its duly authorized agent which issues a financial transaction card.

"Presenting" means those actions taken by a cardholder or any person to introduce a financial transaction card into an automated banking device, including utilization of a personal identification code, or merely displaying or showing a financial transaction card to the issuer, or to any person or organization providing money, goods, services, or anything else of value, or any other entity with intent to defraud.

"Receives" or "receiving" means acquiring possession or control of a financial transaction card or accepting a financial transaction card as security for a loan.

Computer Crime – Hawaii Revised Statutes. § 16-16-20:
Under Hawaii Revised Statutes § 16-16-20, and relevant to the Indictment and allegations in this case, a person commits a Computer Crime offense when he or she willfully, knowingly, maliciously, and without authorization or for an unauthorized purpose directly or indirectly accesses or causes to be accessed a computer, computer system, or computer network for the purpose of devising or executing a scheme or artifice to defraud, or obtaining money, property, or services by means of false or fraudulent pretenses, representations, promises; or committing any other crime.

In this case, the State has alleged a Computer Crime involving the access of Lilikoi's secure financial transaction server to obtain financial transaction cards without authorization.Therefore, in order to prove Mr./Ms. Woods guilty of a Computer Crime, the State must prove the following:

(1) The Defendant directly or indirectly accessed Lilikoi's computer system; and that
(2) Such access was made willfully, knowingly, maliciously; and that
(3) Such access was made without authorization, or was for an unauthorized purpose; and that
(4) Such access was made for the purpose of devising or executing a scheme or artifice to defraud; or obtaining money, property, or services by means of false or fraudulent pretenses, representations, promises; or committing any other crime.

If you find Mr./Ms. Woods guilty of a Computer Crime, you will be asked on the verdict form to determine the amount gained directly or indirectly from the offense.

(3) Presumption of Innocence and Reasonable Doubt:
The Defendant is presumed innocent, and the presumption continues unless, after consideration of all the evidence, you are convinced of the Defendant's guilt beyond a reasonable doubt. The State has the burden of presenting the evidence that establishes the Defendant's guilt beyond a reasonable doubt. The Defendant must be found not

guilty unless the State produces evidence which convinces you, beyond a reasonable doubt, of each and every element of the crime alleged.

"Beyond a reasonable doubt" is defined as "proof of such a convincing character that you would be willing to rely and act upon it without hesitation in the most important of your own affairs."

(4) Evidence – Definition:
Evidence is the testimony received from the witnesses under oath, stipulations made by the attorneys, and the exhibits admitted into evidence during the trial.

(5) Evidence – Inferences:
You should consider only the evidence introduced while the court is in session. You are permitted to draw such reasonable inferences from the testimony and exhibits as you feel are justified when considered with the aid of the knowledge which you each possess in common with other persons. You may make deductions and reach conclusions which reason and common sense lead you to draw from the facts which you find to have been established by the evidence in this case.

(6) Indictments Not Evidence:
Again, the Indictments in this case are the formal method of accusing the Defendant of a crime. The Indictments are not evidence of guilt, and you should not allow yourselves to be influenced against the Defendant by reason of the filing of the Indictments.

(7) Judicial Rulings:
The Court has made rulings in the conduct of the trial and the admission of evidence. These rulings should have no bearing on the weight or credit to be given any evidence or testimony admitted during the trial, nor should they be considered by you in any manner to indicate the conclusions to be reached by you in this case.

(8) Objections:
From time to time during this trial, the attorneys have made objections that I have ruled on. You should not speculate upon the reasons why objections were made. If I approved or sustained an objection, you should not speculate on what might have been said or what might have occurred had the objection not been sustained by me.

(9) Credibility of Witnesses:
It is your responsibility to determine the credibility of each witness and the weight to be given the testimony of each witness. In determining such weight or credibility, you may properly consider: the interest, if any, which the witness may have in the result of the trial; the relation of the witness to the parties; the bias or prejudice of the witness, if any has been apparent; the candor, fairness, intelligence, and demeanor of the witness; the ability of the witness to remember and relate past occurrences, the means of observation, and the opportunity of knowing the matters about which the witness has testified. From all the facts and circumstances appearing in evidence and coming to your observation during the trial, aided by the knowledge which you each possess in common with other persons, you will reach your conclusions. You should not let sympathy, sentiment, or prejudice enter into your deliberations, but should discharge your duties as jurors impartially, conscientiously, and faithfully under your oaths and return such verdict as the evidence warrants when measured by these instructions.

(10) Punishment:
You are only concerned with the guilt or innocence of the Defendant. You are not to concern yourselves with punishment.

(C) Verdict Instructions:

After you have retired to consider your verdict, please select one member of the jury as foreperson and then begin your deliberations. The foreperson is to maintain orderly deliberations but should have no greater influence on the deliberations than any other member of the jury. Your verdict must be unanimous. When you have agreed on a verdict, your foreperson will sign the verdict form, and you will, as a body, return the verdict form in open court.

You will now listen to the closing arguments of counsel in this matter.

(D) Verdict Form:

A copy of the verdict form approved by the Court is attached hereto as Appendix A.

IT IS SO ORDERED, this day of this round of the High School Mock Trial competition.

/s/ Presiding Judge
The Honorable Presiding Judge

	)	SEVENTH JUDICIAL CIRCUIT
	)	
STATE OF HAWAII,	)	COURT OF GENERAL SESSIONS
	)	
Prosecution,	)	
vs.	)	2015-GS-47-0926
	)	2015-GS-47-0927
ELE WOODS,	)	2015-GS-47-0928
	)	
Defendant.	)	
	)	
	)	
	)	
	)	

Appendix A – JURY VERDICT FORM

We, the jury, empanelled and sworn in the above-entitled cause, do, upon our oaths, find as follows:

Defendant is:

COUNT 1 – Financial Transaction Card Fraud – Hawaii Revised Statutes. § 16-14-60

_____ Not Guilty
_____ Guilty

If found Guilty, what is the value of "money, goods, services, or anything else of value" which the Defendant obtained in violation of this statute? $_____

COUNT 2 – Financial Transaction Card or Number Theft – Hawaii Revised Statutes. § 16-14-20

_____ Not Guilty
_____ Guilty

If found Guilty, what is the number of card numbers taken or obtained by the Defendant in violation of this statute? _____

COUNT 3 – Computer Crime – Hawaii Revised Statutes. § 16-16-20

_____ Not Guilty
_____ Guilty

If found Guilty, what is the amount gained directly or indirectly from the offense? $_____

_____
Foreperson

WITNESSES
and
AFFIDAVITS

WITNESS LISTING

PROSECUTION	
Casey Specter	SLED Agent – Computer Crimes
Micah Ross	Roommate
Reese Pearson	Director of Operations - Lilikoi's

DEFENSE	
Dr. Hayden Litt	Computer Engineering Professor
Quinn Bateman	IT Security Specialist
Ele Woods	Defendant

Affidavit of

CASEY SPECTER

1. My name is Casey Specter. I am originally from Honolulu, Hawaii. I am 46 years old. I hold a Bachelor of Science degree in Computer Engineering from Virginia Polytechnic Institute (VPI), but more commonly known as Virginia Tech. After college, I went directly into network security in the law enforcement world. I worked as an analyst first in the Federal Trade Commission (FTC) evaluating safety recommendations for United States corporations conducting interstate commerce electronically. Following three years of increasing case load at the FTC, an opportunity to become a Federal Bureau of Investigations (FBI) agent came open in the newly evolving Computer Crimes Division.

2. Over my ten years at the FBI's Computer Crimes Division, I worked on a variety of cases dealing with breaches of security for individuals, companies, state, and federal agencies. I enjoyed the work and the people I worked with. Early on at the Bureau, I was tasked with saving data and then analyzing the recovered data. It might sound boring, but it was the core of what many cases were based. I then began to find the data people tried to erase or dispose of and determine what it meant. Sometimes, it was simple things such as mob bosses emailing people about who they wanted killed. The more interesting and difficult cases involved professional hackers who stole large sums of money, or spies who used the internet in the trafficking of secrets. For the last type of cases, we worked with the Central Intelligence Agency (CIA), and with the anti-espionage unit at the Bureau. Later on in my career at the FBI, I worked on the front end of cases; establishing if a breach occurred in government systems; and then tracking back to the source of the breach in order to affect an arrest. Most often, once we tracked down a common criminal, they were quick to make a plea to lesser charges, which meant I never had to go to court.

3. I have been back in Luana, Hawaii for the last five years. I came back to Hawaii because of a call I received from my mom. My dad was diagnosed with a type of dementia similar to Alzheimer's. I love my family, so there was no question if I was going to move back home. Thankfully, there was a position at the State Law Enforcement Division (SLED) in the Computer Crimes Division here. It was an easy switch from federal to state work, which allows me to continue my career and help take care of my dad. The position at SLED started in the Internet Crimes Against Children (ICAC) unit. While there, I worked with other taskforce agents to take predators off the street. It is very important work, and often very difficult. It can also be hard on the agents who work the

cases and see the victims of these crimes. Honestly, I was relieved when a transfer inside the Computer Crimes Division allowed me to move back into working financial fraud cases.

4. The case in question deals with a data breach at Lilikoi's. I summarized my investigation in the exhibit marked as Exhibit #4. SLED was notified on September 26, 2015, by Sgt. Harrelson of the Kaimana County Sheriff's Department. The data breach was Far larger and involved more resources than they could handle. With the notification and request from the local agency, SLED took over the forensic portion of the criminal investigation. I was provided with the Kaimana County Sheriff's Department incident report, which has been marked as Exhibit #3. Prior to SLED's involvement, Lilikoi's reported to local law enforcement a data breach of their secure financial transaction servers. More specifically, they reported over 4,000 credit cards were compromised, with 35 Hawaiians' accounts used to make fraudulent purchases through their own Lilikoi's website, starting on September 10, 2015. This information was not used on any sites other than Lilikoi's website. No purchases were made through any in-store locations with the stolen data. In a sense, the defendant was lucky because had there been cards belonging to people from other states, the Interstate Commerce Clause would apply, and it could then become a federal case.

5. Reese Pearson of Lilikoi's served as the main point of contact for the company and also as the main collection point of information for Hawaii's 35 victims. On the afternoon of September 26, 2015, I met with Reese Pearson of Lilikoi's. Working with Pearson made the investigation process simpler from our end, as there were fewer individual reports to take and process. Pearson disclosed to both local law enforcers and SLED about the existence of a contract through West Waiakea University (WWU) to specifically seek out ways to compromise the very systems which were breached. It was reported that five credit cards issued to Lilikoi's were used with permission under the security test contract. It was initially believed that the 4,000 credit cards compromised represented a part of the contract work, and not criminal victimization. This contract, which existed with WWU specifically to breach the security, seemed like a good place to continue my investigation. The professor heading up the contract, Professor Hayden Litt, would provide assistance to determine how vulnerable the system was, so I would have a better idea of what kind of hacker to be identified. The contract between Lilikoi's and WWU has been marked as Exhibit #1. In addition to what I have already mentioned, Pearson clarified some of the things specifically purchased with the fraudulent credit cards. Those items included a 72 inch LED television, one Xbox 360 with three games and two controllers, six

64GB iPads with LTE, one MacBook Pro, and a multitude of other items. Later, we found several of these same items on the inventory list from the search and seizure warrant executed at the on campus apartment of Ele Woods and Micah Ross at WWU. A true and accurate copy of the itemized seizure list has been marked as Exhibit #6.

6. Next, I met with Professor Hayden Litt on September 27, 2015. Litt used an undergraduate student for the purposes of fulfilling part of the contract and felt this was an excellent teaching tool for a bright student. Litt stated there was no way the student, Ele Woods, could have committed the crimes in question based upon the student's character, reputation, and history in the Computer Engineering Department. Litt provided the computer MAC and IP addresses of Ele Woods's laptop used for the purposes of the contract with Lilikoi's.

7. Based upon the information from Pearson and Litt, I began to focus my investigation more closely on Ele Woods. After checking with the WWU Housing Office by way of the West Waiakea University Police Department (WWUPD), I was able to determine that Woods lived in an on campus apartment with a roommate, Micah Ross. A diagram of this apartment, which was the subject of a search warrant, has been marked as Exhibit #7. The next step I took was to interview the roommate, Micah Ross. The WWUPD provided an adequate interview room and Ross voluntarily met with me on September 28, 2015. During the interview, Ross was candid and straightforward. During a follow-up interview with Ross on the afternoon of September 29, 2015, at SLED's Computer Crimes Division, Ross answered additional questions as to packages in the apartment, and knowledge of a file containing credit card numbers. To be sure Ross was providing truthful information; I also obtained a copy of Ross's and Woods's Fall 2015 class schedules from the WWU Registrar's Office. An accurate copy of those schedules has been marked as Exhibit #11. Ross confirmed the class schedules in the follow-up interview. Ross mentioned many packages came into the apartment, but could not specify when they arrived. Ross also talked about a 72 inch widescreen TV, which was supposedly one of Woods's birthday presents. The television matched one of the items from the fraudulent purchases. By this point, I was certain Ele Woods was the hacker I was chasing.

8. Following the interviews with Pearson, Litt, and Ross; I conducted an analysis of Lilikoi's servers. Several interesting things came from this portion of the investigation. There were multiple attempts made by computers outside the Lilikoi's system to access secure elements both to the corporate website as well as the secure financial transaction server. At least three of those attempts to breach the secure elements

of the corporate website were successful, and changes were made to the content of publicly displayed pages. As per the contract, I knew this was an approved activity. As the corporate website did not concern my criminal investigation, I did not follow up with ascertaining who made those breaches. One computer was identified by IP and MAC addresses as responsible for all the attempts to breach the secure financial transactions server. An IP address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network. The IP address traced back to WWU. The MAC address, which is media access control address (MAC address), identifies where the computer is on a physical network. The MAC address matched to the information submitted to SLED by Professor Litt, specifically to the violating computer owned by Woods. Based upon IP address reports, MAC address information, and the information provided by Professor Litt, I secured a search and seizure warrant seeking specifically the computer in question used to commit the crimes, as well as any information relating to the crimes, and finally any items on the list provided by Lilikoi's of fraudulent purchases matching the IP address marked as Exhibit #10. The order history query provided by Lilikoi's based upon the specific IP address provided a list of order numbers, order dates, order times, purchaser names, items purchased, number of units purchased, a shipping address, the last four digits from the credit cards used, the total purchase price, and the shipping status.

9. In preparation and as a courtesy, WWUPD was notified of the search warrant. A true and accurate copy of the warrant has been marked as Exhibit #5. WWUPD officers assisted SLED with the execution of the warrant on October 3, 2015, at Apartment 230 South Quad, by providing officers on scene, and by securing key access from the WWU Housing Office. From the common areas of the apartment, SLED agents seized an Xbox, several games, and a 72 inch LED television. The items seized matched the description list provided by Lilikoi's. In the bedroom marked as Ele Woods's on Exhibit #7; a true and accurate copy of the apartment diagram; a Hewlett Packard (HP) laptop with MAC address matching the warrant specification was located on the desk, and seized. Next to the laptop, in plain view, was a file folder containing a print out of all the credit card numbers pulled from the data breach at Lilikoi's, which was also seized. Finally, under the bed in Woods's room was one iPad 64GB LTE device, still sealed in the packaging, and matching the description on the warrant. Only three shipping labels were retrieved from the trash can in the common area of the apartment and also entered into evidence. One shipping label was addressed to "Ele Woods," one to "Student," and the other was to

"WWU Student." An accurate copy of all shipping labels found has been marked as Exhibit #8. No items in question were found in the bedroom marked as Ross Micah's. Though an external door lock and deadbolt were present on the exterior door, no locks were present on either bedroom doors. No suspects or other students were present in the apartment when the warrant was executed. The diagram in Exhibit #7 was provided by the WWU Housing Office and is a true and accurate depiction of the on campus apartment. Based upon the layout of the apartment, and the amount of personal effects strewn throughout, it was impossible to determine to whom any of the items in the common area specifically belonged. Prior to securing and exiting the apartment at the conclusion of the search, a copy of the warrant and a copy of the itemized seizure list were left on the table in the kitchen area.

10. Forensic examination of the laptop revealed Ele Woods as the owner. The laptop did not have a startup password or an operating system password. There were no fail-safes, trap doors, nor hidden files of note. Fail-safes in this context are a type of additional security provision in which after logging onto the computer, one must complete an action or series of actions to prevent a lockout and reformat of the hard drive. For a student who majored in computer engineering and had a course load dealing in network security, certainly individual computer security did not appear to be a priority. Prior to poking around on the computer, I utilized custom forensic software back at the SLED offices to clone the drive – that is, to make an exact backup of the laptop's hard drive. The custom recovery software makes use of certain algorithms to recreate missing bits of data from intentional attempts to erase data. Algorithms are a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer. In this case, the recovery function was not necessary. Copying the hard drive also preserved the original hard drive. This is very important because if the agent was looking at the original drive and made a change to it, then the evidence would be considered tampered with and thus inadmissible in court. The forensic investigation was carried out on the forensic copy of the hard drive while the original hard drive remained in evidence. From a simple history search on the web browser, it was determined that this was in fact the computer used to violate Lilikoi's security.

11. Based on the information gathered in the interviews, the search and seizure warrant, and the forensic examination of the Lilikoi's servers as well as Woods's laptop; I took Woods into custody on October 4, 2015. Following Miranda warnings, I questioned Woods about the crimes in question. Essentially, I was providing Woods the opportunity to

explain the other side of the story. Woods denied any involvement in the illegal aspects of the computer use but admitted to breaching the server at Lilikoi's and collecting the card data. Woods declared the data breach was done as part of his/her contractual work with Professor Litt. During the interview, Woods again denied breaking any laws and invoked his/her right to counsel, the interview ended, and Woods was transported to the Kaimana County Detention Center. Woods kept saying “it was only some chewing gum” and “I cannot Believe this is happening over packs of gum.” Shortly thereafter, I was called before the Grand Jury by the Solicitor’s Office. Following my testimony, Woods was indicted for the charges stated in the Indictments.

WITNESS ADDENDUM

I have reviewed this statement, and I have nothing of significance to add at this time. The material facts are true and correct.

Signed,

Casey Specter

Casey Specter

SIGNED AND SWORN to me before 8:00 a.m. on the day of this round of the High School Mock Trial Competition.

Anthony Roberts

Anthony Roberts, Notary Public
State of Hawaii
My Commission Expires: 10/24/18

1. My name is Micah Ross. I am 22 years old. My birthday is September 5th. Both Ele and I have September birthdays, an interesting coincidence. I am finally out of school, although I never thought I would get finished with all this crazy stuff involved with this case. Even with everything going on, I was able to graduate early because of all the summer classes I took. I grew up in Hawaii, and have always known that I wanted to work with computers. I do not have a job yet, but I am sure I will get picked up by a good company soon.

2. The fall of 2015 was when all of the hacking case stuff started. Fall semester started on August 15, 2015. Ele Woods and I were roommates at West Waiakea University (WWU). Both of us were juniors in the computer engineering program, so it made sense for us to be roommates. We were roomies and sort of friends. I wanted Ele as a roommate more because of the weird hours we were working in the computer labs more than anything else. I have had other college roommates who were liberal arts majors – you know art, music, history, etc. They did not understand the amount of studying we have to do and why we have to be in the lab versus studying and playing back at the dorms. Neither of us ever really went home on the weekends, because there was always so much studying to do, not just to keep up, but to get ahead. Ele and I were taking summer classes, so we took over apartment 230 in the South Quad building the first week of May 2015. A diagram of our apartment was provided by the WWU Housing Office has been marked as Exhibit #7.

3. Apartment 230 in South Quad was the perfect place for students like Ele and me. It was a three or four minute walk at most from the apartment to the Cannon building with all our classes. Ele and I were in some classes together down in the Cannon engineering building during our freshman and sophomore years. My previous roommate was a history major who never studied, and that annoyed me. Ele's roommate graduated his/her sophomore year. Since neither of us had a roommate and we were both in the same program, it kind of made sense to snag one of the on campus apartments together. I figured there would be much less struggle over things since we were roughly on the same time table. Our schedules did not quite match up, so we were not always in the same place at the same time. We both had lab listed for our major, but computer engineering students do not have a set time to be in the lab. The computer labs are open around the clock. A copy of our fall schedules has been marked as Exhibit #11.

Ele and I got along okay in the beginning of summer semester. As things went on, I think we both got more and more annoyed with each other. Some of it was probably because we were not great friends before that school year and the only thing we had in common was our major. Our lack of friendship became more apparent as the semester continued and the realization was there that we were never going to be best friends. Ele could be so selfish and uncaring about other people and their wants. Sometimes, I felt like Ele was Sheldon and I was Leonard on *The Big Bang Theory*. Ele forever had rules about food, rules about when people could and could not be at the apartment, no one was allowed in his/her room, and rules about never touching Ele's laptop – like I really cared anyway. Once September rolled around, we really were not speaking much at all. We only saw each other at the apartment and in class. Occasionally, we sat and watched TV in the evenings. When Ele did work in the common areas s/he took up so much space s/he hogged the whole common area.

4. Ele and I were both very interested in cyber security and in particular the security of business servers. I thought it would be a great career path, because somebody is always going to try and hack into computers to get stuff. Ele was better at hacking than me, which is why Dr. Litt picked Ele to work on Lilikoi's security analysis. Certainly, Ele never told me s/he was picked to work on the project, but it was not hard to figure out. There is a lot of secrecy inside the computer engineering program and with secrecy comes snooping. Students do not talk to one another about projects with different professors, because it gives a better advantage before graduating. Call it resume building, if you will. Competition is good.

5. Early in the fall semester, Ele seemed more erratic than ever with the late night comings and goings, turning the laptop computer away from me anytime I walked by in the common area, and overall being more secretive than normal. Around this same time, random packages of all sizes started showing up at the apartment. I did not think much of it at first. The first package I saw open contained several packages of chewing gum. Soon after, a few more of the exact same sized boxes arrived, but I never saw them opened. I do not remember how many boxes there were. Some of the shipping labels were part of what was seized. I recognize the labels that were marked as Exhibit #8. Over the next several days, more boxes arrived. Then came the really big box. Ele got a 72 inch LED TV for his/her birthday. The TV was an outstanding present to say the least. We were the envy of everyone else in South Quad, and when I hooked the Xbox 360 up to it, everyone wanted to stop by and play games. It was really kind of cool that Ele did not

care about the TV at all. Everyone else seemed to like it, but Ele largely ignored us and continued with whatever was on the laptop. Ele always got big packages. Mr. Woods, Ele's dad, is a big wig with some federal defense contractor. I know Dr. Litt is always asking in and out of class how business is for Ele's dad and suggesting we could all possibly work on a contract together for Sterns Consulting. Apparently, Dr. Litt could make a lot of extra money if Mr. Woods's company would ever contract with him/her and WWU.

6. Finally, curiosity got the better of me one day and I ended up looking at the papers surrounding the laptop in Ele's room. Ele had what looked like 20 or more pages of nothing but numbers in a file folder. At first, I thought it could have been some sort of computer algorithm Ele was trying to figure out from the advanced numbers processing class we were both taking (but in different sections). Then I realized what the numbers were. The numbers were 16 digit credit card numbers and expiration dates. I got nervous, and immediately walked out of Ele's room and away from the papers. Ele must have stolen the numbers from a server. I was not going to jail for Ele's hacking. I then began thinking about all of the packages coming in like the gum and the huge TV. It was all starting to make sense. Ele had to be making online purchases using the credit card numbers in the folder. I did not know where the purchases were coming from, but I wanted no part of it. Hacking and stealing can ruin a career before it ever gets started! I never wanted to be what they call a "Black Hat," or someone who hacks and creates chaos on the web. I want to be a "good guy," a "White Hat" computer and cyber security specialist who protects systems from hackers. I was really torn about turning Ele in or keeping quiet about the whole thing. Hawaii does not have a law requiring me to report if I know a crime happens, just that I cannot lie to the police if they ask me about a crime.

7. Before I could tell Ele to stop hacking and buying things for our apartment, SLED showed up along with the West Waiakea University Police Department (WWUPD). They interviewed me at the WWUPD on September 28, 2015. Agent Specter gave me a card and said I needed to think about my options, which were to either sit at the defense table or the prosecution table. Agent Specter told me things were far more comfortable at the prosecution table. Agent Specter ended the interview and I was told I could leave, but to think carefully about my options. I called SLED the next morning, September 29th, and set up a meeting for that afternoon. It really was not as grueling or tough as I thought it would be or anything like what you see on TV. Agent Specter was very nice to me. We met in a big conference room at a SLED building off of Bush River Road. I

told Agent Specter what I had seen on the desk around the laptop in Ele's room, and where I thought all the new things in our apartment had come from. Agent Specter asked a lot of questions about specific items coming into the apartment and if I could remember when exactly each package arrived, or who each one was from. I did not have all the answers. The interview took quite a while. At the end of the interview, Agent Specter told me I could not discuss the interview with Ele or of having met with SLED. If I did, I would be charged with interfering with a lawful police investigation or, even worse, charged with accessory to crimes.

8. A couple days after my SLED interview, SLED got a search warrant and took all sorts of things from our apartment. Luckily, I was at class when the search happened. I do not think being present when your apartment was raided by SLED would have been any fun at all. According to the seizure list marked as Exhibit #6, on October 3, 2015, SLED took the TV, the Xbox, an iPad, Ele's computer, and all the notes and files next to the computer. It really was not fair – SLED took the Xbox. The Xbox and the TV were the best things about our apartment. The police left the seizure list on the dining table beside a copy of the warrant they served while we were gone. A copy of the warrant has been marked as Exhibit #5.

9. Once SLED raided our apartment, Ele was nowhere to be found. I guess that is what happens when someone is on the run from the law. Ele ended up getting arrested and charged with everything relating to the hacking at Lilikoi's. After things subsided from the arrest, I ended up in the apartment all by myself for the rest of the school year. It was pretty cool to have the place to myself and not worrying about all of Ele's rules and stuff all over the place. Not to mention, I was able to finish up the school year on time and in peace. Agent Specter was not kidding. It is much easier to be at the prosecution table.

[Micah Ross's Witness Addendum is on the next page.]

WITNESS ADDENDUM

I have reviewed this statement, and I have nothing of significance to add at this time. The material facts are true and correct.

Signed,

Micah Ross

Micah Ross

SIGNED AND SWORN to me before 8:00 a.m. on the day of this round of the High School Mock Trial Competition.

William Smith

William Smith, Notary Public
State of Hawaii
My Commission Expires: 12/08/19

1. My name is Reese Pearson. I am currently the Director of Operations for Lilikoi's. I am 39 years old. Prior to this job, I was the Security Operations Director for Lowe's. During my time there, I oversaw the improvement of the transaction card processing systems and evolution to the newest generation of Point of Sale (POS) machines. I received my Bachelor of Arts degree from Furman University and my Masters of Business Administration from Vanderbilt University.

2. Lilikoi's is a Hawaii based retail operation with 12 stores in the state. Our corporate office is here in Kaimana, Hawaii. We are what one might call a general merchandise retailer. We operate very much in the same way as Target or Wal-Mart, but quite a bit smaller. We also have the added benefit of being able to stock many more "Made in the USA" and Hawaii specific items. For example, many of the clothes and linens we sell are sourced right from Hawaii.
Where possible, the fruits and vegetables are local or at least come from the United States. As a growing chain store, imagine the volume of electronic transactions we conduct on a daily basis – almost no one carries cash anymore. I would estimate less than 15% of our annual business is conducted via a cash transaction. With 85% of our electronic business from our brick and mortar stores and the website, I am always concerned for people who want to rob our company. I am not referring to "rob" in the traditional sense. I am referring to hacking our servers. To me, a hacker is no better than someone coming in a store with a pistol and a ski mask demanding money. A hacker is stealing plain and simple.

3. With the increased hacking and embarrassing stories everyone hears about state and federal government data breaches, I tried to be proactive. In February of 2015, I went to Professor Litt at West Waiakea University (WWU) and offered a contract to test Lilikoi's security vulnerabilities, both in our stores and online. Professor Litt came highly regarded and recommended based upon prior work with the US Department of Defense (DoD). While at DoD, Professor Litt was tasked with searching for weak points in our nation's military networks.

4. Based on the professor's experience and knowledge, Lilikoi's reached out via the WWU Office of Grants and Research to evaluate Professor Litt's availability. To say it was a long process is an understatement. I began by asking whether the professor was available and inquiring about what needed to happen for the process to take place.

After filling out a huge stack of forms for the University, Lilikoi's was able to submit a request for contract proposal to Professor Litt. I intentionally did not include Lilikoi's IT Director or IT Services Department in this request. I felt the IT Department had become complacent in their processes and policies. I needed to see how those processes and policies would stand up to real world attempts. Besides, if I told them in advance of an impending hacking attempt, they would have changed or tightened policies in advance. Without them notified, I could test our actual level of readiness.

5. Specifically, our request asked Professor Litt for an evaluation of our electronic safety in stores and online. I received back a mostly acceptable proposal. I did not care for the amount of indirect costs the University was proposing to charge, but it was non-negotiable. I also did not care to allow Professor Litt to use graduate students on the project. I preferred a much tighter control over who was conducting the work. I believe I specified my preference in an email with Professor Litt, but I looked for the email and I must have deleted it. I worked with our legal department to modify and firm up the contract, which was sent back to WWU. We deleted the line from the original proposal that specifically allowed a student assistant on the project. I see now, after the fact, we did not delete the funds for the student assistant position. Apparently, Professor Litt believed it was okay to simply add back the student position – clearly not acceptable. The contract was signed by the University and Professor Litt. The contract was through WWU and specific to Professor Litt, as we did not want any other people to be involved in the hacking process. The contract was accepted and signed by all appropriate parties. The contract was executed July 25, 2015, with the expectation of the contract work beginning within 30 days and terminated automatically on December 31, 2015. A true and accurate copy of this contract has been marked as Exhibit #1. Likewise, the Non-Disclosure Agreement (NDA) required by Lilikoi's has been marked as Exhibit #2.

6. The terms of the contract were very explicit as to what was acceptable and what was not. Professor Litt could use any commercially available and viable computer equipment s/he wanted. Professor Litt was directed to look at three different processes. First, there would be an attempt to breach electronic security in a random cross-section of ten store locations. This would include checking for unsecured WiFi access and unsecured terminals in which information or purchases could be made without paying for them. Second, there would be an attempt to breach the security on the corporate website in order to make changes to certain web pages, which changes were agreed upon in advance and sufficiently far into the website that normal users likely would not encounter the

inconsistencies. Third, Professor Litt was to attempt to breach our secure financial transaction servers. If successfully breached, there were five particular credit cards (all issued to Lilikoi's) to be used, if found while conducting the server breach, for random online purchases. The total purchases allowed were to be no more than $50 per card. If a breach was possible, an electronic trail proving the time and location of the breach would be provided to show us at Lilikoi's which weak spots needed improvement.

7. On the morning of September 26, 2015, James Myrick, Lilikoi's Director of IT, demanded an emergency meeting. He informed me Lilikoi's was under cyber-attack. I asked for further details. I was provided with a list of suspicious purchases all made with different credit cards but shipped to the same address. It is outside of normal practices for so many different cards to all have the same address, which set off a security warning. Once the security system was triggered, Myrick ordered all of the servers to be checked. The check revealed numerous unauthorized attempts to open ports on the server. As a result, a successful security breach was made on a server housing sensitive customer information. In addition, a check of the website showed changes to the corporate page. Based upon the checks of the systems, a report was generated showing one IP address responsible for all illicit purchases, which has been marked as Exhibit #10. I recognized this website change as it had been agreed upon as part of the contract with Professor Litt. I identified five of the cards used for purchases as Lilikoi's corporate cards authorized for use under the contract with Professor Litt. The problem was Professor Litt was only contracted to use the five credit cards identified as belonging to Lilikoi's if the breach was successful; yet another 35 credit cards were used. The result was the theft of Lilikoi's merchandise and fraudulent charges to unsuspecting victims. At this point, I informed Mr. Myrick about the contract with WWU and what the contracted items were.

8. Since this breach exceeded the five pre-determined credit cards contracted, we called the police immediately to report the data theft. The police arrived in a reasonable time, but this case was too complex for local authorities. Within 30 minutes of coming to Lilikoi's corporate offices, Officer McCabe with the Kaimana County Sheriff's Department requested a detective to conduct the investigation. Sgt. Harrelson followed up with our office long enough to determine this was outside the scope of what her agency could handle. Sgt. Harrelson called the State Law Enforcement Division (SLED) to seek further assistance. Agent Casey Specter with the SLED Computer Crimes Division took over the case the same day. Lilikoi's was provided a copy of both the original incident report, which has been marked as Exhibit #3; and the SLED report, which has been marked as Exhibit

#4. I was interviewed especially relating to the contract we had with Professor Litt. I provided thorough access to all of our servers for the forensic evaluation. Agent Specter kept me informed throughout the process. I was pleased to see an arrest shortly thereafter, not to mention recovering some of the items bought fraudulently. The people who had their credit cards fraudulently used, received a credit almost immediately by their individual issuing card companies. Those issuing companies in turn charged the losses to Lilikoi's. Because fraudulent purchases are the same as if someone walked into a store and stole items off the shelf, the police returned the recovered items to Lilikoi's, the victim. Lilikoi's will most likely list the recovered items as “Open Item Sales” in a local store following the conclusion of the trial. We usually sell opened items at 25% off of the original price. This way, Lilikoi's can at least recoup some of the value from the stolen items recovered.

9. Even though the results of the contract ended up going horribly astray, many good things did come out of the hacking. We were able to identify several electronic security vulnerabilities at the store level. Specifically, Professor Litt found several store managers and assistant managers were using unsecured wireless routers, which opened up our local network to anyone with a Wi-Fi access via computer or even tablet. We have since changed our protocol on how local stores operate their network, updated the training for managers to include internet safety concerns, and Lilikoi's now has an IT Manager not assigned to any specific store, but rather with the job of continually checking all of our stores for this type of vulnerability. Further, we changed the amount of idle time before security lock out engages on all of our order guns and sales terminals company wide. Clearly, we found the online shopping process had at least one severe security problem. Fortunately, these were things our company could move aggressively on in order to make our company much safer and more trustworthy. We wanted to restore our customers’ faith in Lilikoi's. Now our online process is on par with the most robust electronic retailers in the industry. The new online purchase portal has a two-step authentication for logging into accounts, all electronic payments go through a new security portal, credit card data is broken up before storing, and we have implemented the CVV requirement (using the three numbers on the back of the credit card) on all electronic purchases.

10. Having said the good things resulting from this breach, let me tell you the bad things that happened. This attack on Lilikoi's cost over $10,000 in fraudulent charges, which was essentially stolen merchandise. When fraudulent purchases happen, the credit card companies take the money back from the vendor who allowed the purchases to happen in order to reimburse the victims, which hurts our bottom line. Many of the items we

sell have such a small margin of profit on them in order to be competitive, that one stolen item can wipe out the profit margin of selling as many as 100 or more.

11. Because of this breach, we had to release a public statement about it, which caused affected consumers to replace their credit cards. The public image from the announcement and the feeling from the public was that we could not keep their transactions secure. And since our statement was released on an otherwise slow news day, the security breach was the lead story on most network news channels that evening. The reality was the exact opposite. We were proactive and hired someone to evaluate the potential for a breach. As soon as the breach was found, we had programmers recoding to close the security hole. Fixing the breach made us a stronger company and a safer online presence. Unfortunately, the public perception is the reverse. Far worse than the initial financial hit, was the following wave of lost revenue once the story of the computer breach went public. This wave of lost revenue was a direct result of reduced confidence from the community. Sure there were only 35 actual victims in Hawaii, but there were over 4,000 credit cards actually put at risk. Those 4,000 potential victims told their friends they were actual victims, and then those people told people they knew, and soon the belief was that there were massive numbers of people with their identity stolen from them by doing business with Lilikoi's. The poor public image has hurt the bottom line far worse than the initial hacking and fraudulent purchases.

12. In the time since the publicity surrounding the hack, we had about a 5% increase in our cash transactions in the brick and mortar stores. You might say the increase was good, but we also saw a nearly 30% drop in our online sales and a 15% drop in our brick and mortar card transactions. To say people were and still are skittish of using their credit cards to buy at our stores is an understatement. To entice people back into our stores and online, we have had numerous days where we offered an additional 10% off everything in our stores and online. The incentive worked pretty well, but not enough success to offset the overall losses. To put this in perspective, Lilikoi's may have to lay off employees, or schedule employees for fewer hours due to lower staffing needs.

13. Not only has Ele Woods hurt the company itself, but also the many fine people working for Lilikoi's trying to earn a living. Ele Woods has cost Lilikoi's a great deal of money, time, and stress. Professor Litt also cost Lilikoi's money because s/he decided to violate the terms of our agreement. Professor Litt brought in an undergrad who took what s/he knew and used it not to make our company better, but to tear at it from the inside. I think Ele Woods should do serious jail time and I can assure you Lilikoi's

will never utilize Professor Litt or West Waiakea University again. I am going to do everything in my power to make sure Professor Litt never gets a private sector security contract again.

WITNESS ADDENDUM

I have reviewed this statement, and I have nothing of significance to add at this time. The material facts are true and correct.

Signed,

Reese Pearson

Reese Pearson

SIGNED AND SWORN to me before 8:00 a.m. on the day of this round of the High School Mock Trial Competition.

C.H. Gallant

C.H. Gallant, Notary Public
State of Hawaii
My Commission Expires: 12/5/17

Affidavit of

DR. HAYDEN LITT

1. My name is Dr. Hayden Litt. I am a tenured professor of Computer Science and Engineering at the West Waiakea University (WWU). My office is located in the Cannon building, where all the computer engineering courses are held. I specialize in network security and electronic transaction security. I earned my Bachelor of Science degree in Computer Science from Ohio State University. I later completed my doctorate at Massachusetts Institute of Technology (MIT). Back then, the field of computer engineering was simply a part of computer science. As things have evolved over the years, the field has been divided into two separate fields of study – computer science and engineering.

2. Over the years, I have done extensive consulting work for the Federal Bureau of Investigations (FBI), the U.S. Department of Defense (DoD), and Visa. This consulting work was of a sensitive nature, and all of it revolved around making systems as secure as possible – essentially making them hacker proof. One of my tasks included searching for weak points in the military's network. I am sure all of my consulting work combined helped me secure tenure at WWU. Since those contracts, contracting work with private companies looking to make their web presence more secure has increased.

3. I have had both Ele Woods and Micah Ross in many of my courses during their time at the University. Micah was an average student, but Ele was truly gifted with computers. It was almost as though Ele could visualize the network pathways and what the vulnerabilities were. As I said, very gifted, perhaps even as good as I was as an undergraduate student. As such, I often engaged Ele in smaller parts of University projects and contracting work for which I was responsible. In the fall semester of 2015, Ele took both the Professional Issues course and Systems Engineering course that I taught. Micah Ross was in the Professional Issues Course only. I have looked at the class schedule for Ele Woods and Micah Ross marked as Exhibit #11, and it is a true and accurate copy.

4. In February 2015, I was approached by Reese Pearson, Director of Operation with Lilikoi's. Lilikoi's was interested in engaging me on a contract to seek out electronic security risks within their servers, brick and mortar stores, and website. I asked for a few further details and then told Pearson I would put together a proposal detailing the hours, number of researchers, the University's indirect costs, and any equipment needs for submission and discussion with Lilikoi's. Within a ten day window, I compiled all the costs

and submitted the proposal to Lilikoi's by way of the Office of Grants and Research. Though the contract and work would be performed by me, all such projects must go through the proper channels at the University. This ensures the Office of Grants and Research gets their cut through the additional percentage fee called indirect costs. These indirect costs help offset instructors to cover my classes – if needed, equipment needed from the University, keeping the lights on and other administrative things. Thus the contract from Lilikoi's would go through the University and then to me. Likewise, Lilikoi's payment for the contract went through the University and then to me.

5. Following my response to Lilikoi's, neither I nor the WWU Office of Grants and Research heard anything for several months. It is quite common to have a corporate request and then not hear back for a while. It can be due to a number of factors from the company deciding an endeavor was too costly, changes in leadership, other corporate burdens, getting hung up in the legal department for review, and so on. Finally in July 2015, Lilikoi's responded to my submission. They agreed with all aspects of my proposal except for one. In the email from the Director of Operations, “Lilikoi's would prefer that the contract be handled by Professor Litt without the use of graduate students.” I found that statement to be a ludicrous request given the amount of work requested and the timeline to complete the contract. Perhaps more importantly, I took note of two aspects of their sentence “Lilikoi's would prefer” and “graduate students.” I would “prefer” to have a hacienda on the coast of Spain, but that does not make it so. And, I do not typically engage graduate students on these types of projects, as they have practical projects of their own while working towards their graduate degree. However, undergraduate students do not have such large projects, and are excellent choices for the mundane aspects of contract work. The contract, marked as Exhibit #1, was signed by all parties on July 25, 2015. The contract is a true and accurate copy. Interestingly enough, Lilikoi's did not eliminate the money for a student working on the project from the approved budget. In looking at their preference and evaluating the best way to complete the contract as presented to WWU, I chose to have an undergraduate student work with me on the project.

6. In the approved contract with Lilikoi's, I was directed to assess the electronic security of Lilikoi's in three ways. First, I was to attempt to breach the network in individual stores by looking at the vulnerabilities of unsecured terminals, product ordering tools, and unsecured Wi-Fi hotspots within stores. For this, I was to take a random sample of ten stores. The second prong of the evaluation was to look at the corporate website. More specifically, I was directed to attempt a breach on their corporate website. To

substantiate this process, several pages deep within the site architecture were designated for me to make changes. These pages were designated because they were sufficiently deep inside the site so the average user would not stumble across strange information on the Lilikoi's corporate site. The final part of the evaluation and the reason we are here today, dealt with the security on the financial transaction servers. The contract specifically directed me to attempt to breach the secure financial transaction servers in order to gain access to user account information. This user information could include, but not be limited to, names, addresses, user ID's, and most importantly credit card information. If successful in this breach, five credit cards issued to Lilikoi's would be in the customer database, which were identified in the contract with their last four numbers. Those credit card numbers were to be used to make purchases on the Lilikoi's website, if possible. No more than $50 was to be spent on each of the five credit cards.

7. I could not think of a better student to work on this project than Ele Woods. With Ele's analytical mind and excellent abilities in networking, I was certain Ele would be an asset to my evaluation. Following the Professional Issues class on Wednesday, August 21, 2015, I asked Ele to stay behind. Once everyone left the classroom, I closed the door and asked Ele if s/he would have any interest in working on a new security contract that I acquired for the University. Of course the answer was yes. What student would not want to work on a project with me? I discussed the aspects of the contract with Ele and swore him/her to secrecy, which is common with these types of projects. I told Ele to drop by the Grants and Research Office later to sign the Non-Disclosure Agreement (NDA). NDA's are the legal way of swearing someone to secrecy on a project. Exhibit #2 is a true and accurate copy of my signed NDA with Lilikoi's. I did not get a signed NDA from Ele as this was really just a paperwork issue, and not something I concern myself with.

8. The first part of my evaluation led me to a random sampling of Lilikoi's stores. I determined that all ten stores evaluated were very lax in enforcing security policies. I was able to gain access to unsecured terminals in seven of the ten stores. These terminals were not just Point of Sale (POS) devices, but computers with full access to the store systems. I was able to insert myself in as a customer who was waiting on back ordered merchandise, and I managed to change the price on certain items I could see were back ordered. In all ten stores, there were unsecured ordering tools (commonly called a scan gun). Scan guns are dangerous to leave unsecured as they can control ordering amounts of items for delivery to the individual store, and can adjust prices for items going

on sale. If a scan gun is used improperly, a person could significantly discount a product and then it would ring up for an incorrect price at the POS machines at checkout. With this access, someone could walk out with items paid for way less than originally priced. Finally in two of the ten stores, I found unsecured wireless routers plugged into data ports. With these unsecured access points I was able to login and make myself an employee, set up payroll, and process myself to have two back paychecks owed to me. Clearly, these were not checks I was going to pick up, but the existence of such checks did make the vulnerability very clear.

9. The second part of the contract was breaking into the corporate website and making changes to the pages they noted, which was very easy. Their Content Management System (CMS) was pretty easy to guess. Once I could get to the CMS, it took a simple hacking program available on the web and I was in Lilikoi's system within about 45 minutes. As it turned out, Lilikoi's used a simple password system with letters and numbers. The password was not case sensitive, it did not rotate on a monthly basis, it did not require using more than seven letters/numbers in the password, and it did not allow for the use of ASCII characters (such as @#$%*&). All of those things would have made it much harder for the computer program I was utilizing to gain access to their servers.

10. The portion of the contract I offered Ele the opportunity to work with me on was the third and final component of the contract. In truth, I did not think Ele would get any further than identifying the secure financial transaction servers and perhaps get into some individual user data, as typically user names and addresses are not as robustly protected as actual credit card data. Surprisingly, Ele was able to break into Lilikoi's system, retrieve thousands of credit card numbers, identify the five agreed upon credit card numbers, and buy chewing gum with those identified credit cards. Shame on Lilikoi's if an undergrad could break into their system in a mere matter of days.

11. I had not completed the second full phase of the contract before Ele came to me with results of his/her efforts on the afternoon of September 23, 2015. Ele strolled into my office, and dropped probably ten to fifteen packs of chewing gum on my desk. Very smugly, Ele told me s/he liked gum and Lilikoi's was kind enough to buy all the packs now sitting on my desk. I was pleased with Ele’s success and we had a great discussion for the next hour or so about the ins and outs of the data breach and what information was recorded. Ele told me there was a paper file back in his/her campus apartment documenting how the breach was carried out, a list with all of the compromised

credit card numbers, and the information on the purchases with Lilikoi's five credit card numbers specifically issued to Lilikoi's.

12. I instructed Ele to secure all the documents and turn them over to me. When Ele started the project, I did receive the MAC Address and IP Address for Ele's personal laptop. Prior to Ele turning over the documentation of the breach to me; SLED seized Ele's research from the campus apartment of Ele and Micah Ross. Though I have tried for months, none of the legitimate research information was released by SLED. SLED's refusal to release information left my research incomplete. As such, I did not receive full payment for the contract. I believe the University and Lilikoi's are in litigation over the terms and completion of the contract, but the litigation is outside the scope of my job.

13. Reese Pearson with Lilikoi's was very upset about the data breach beyond the scope of the contract and everything that has happened since. I cannot say it surprises me that Reese Pearson would be upset. It is incredibly embarrassing to have a college student expose a company's vulnerabilities. Truly, it is tragic that someone stole the data in Ele's possession and used it for ill will. I do not believe for a single moment that Ele was the one who made the illegal purchases. Furthermore, I do not see how Ele could be charged with all of these offenses, when clearly the work was being carried out at Lilikoi's request.

WITNESS ADDENDUM

I have reviewed this statement, and I have nothing of significance to add at this time. The material facts are true and correct.

Signed,

Dr. Hayden Litt

Dr. Hayden Litt

SIGNED AND SWORN to me before 8:00 a.m. on the day of this round of the High School Mock Trial Competition.

Miriam Wrenn

Miriam Wrenn, Notary Public
State of Hawaii
My Commission Expires: 12/08/20

1. My name is Quinn Bateman. In December, I turned 38 years old. I have lived all over the country. Sometimes I lived on the grid and sometimes off the grid. Truthfully, I prefer to be off the grid, which is so much easier. I am currently the owner and principle agent of Gray Hat Consulting located in Alexandria, Virginia. Anyway, I grew up in the Washington DC area. My parents were both contractors with the U.S. Department of Defense (DoD). My dad got me into computers at an early age. He was one of the contractors behind the design and build of the Cray 2 Supercomputer – and that was really cool. A Cray 2 Supercomputer in its day was to computers like the Lockheed SR-71 was to other jets of its day – both were really fast and powerful.

2. After an early start with my dad teaching me what he knew about supercomputers, I knew computers were for me. I did very well in high school without trying. After high school, I applied to and was accepted into the Electronic Engineering program at Stanford University. Stanford was a great place to be and they were famous for pranks on campus, especially in the engineering programs. But if one prank went bad, they asked you to leave quickly. I set up one of my classes to have the manipulator arms (big industrial arms used for manufacturing) to dance to the sound of the professor's voice. Unfortunately, it shorted out and caused a small fire and about $25,000 in damages. Stanford "invited" me to try out other opportunities outside of academia after the mishap. I left Stanford and never looked back.

3. I am a reformed Black Hat. Before most of you knew what the internet was, I was out there compromising systems and making money. A Black Hat is someone who can break in and take things electronically for financial gain. Anyway, after leaving Stanford, I bummed around staying with one friend after another. I wrote some code as an Apple consultant for a little while and was really bored with the job. Eventually, some friends invited me to a Black Hat convention, which was a chance to learn about underground computing. There was everything from people creating viruses to people interested in taking down and holding the entire internet hostage. Needless to say, I was in my element. Ultimately, I started working with different people who were into financials. This is to say we worked on getting inside the big banking systems and taking money. One hack in 1999 that got me noticed by the Federal Bureau Investigation (FBI) was when I got inside Merrill Lynch. Once I was inside, I set up my own account. My account looked and acted like a real

bank account. What I did to fund my account was shave one cent off every transaction Merrill Lynch did via the New York Stock Exchange (NYSE). The hack was a brilliant bit of computer manipulation, and I was a millionaire within a couple of weeks. It is really amazing how many transactions actually happen daily.

4. Well as it turns out, the FBI caught on to my little project and I was caught eventually. The agents were impressed with my knowledge and code writing abilities, not to mention the fact that I knew just about everyone in the hacking world at the time. They offered me an opportunity and I could not say no. I could either go to prison for the full term of the 15 year conviction they knew they were going to get, or I could cooperate with them and become a ward of the feds for ten years. They would be responsible for me, and I would get a salary with a job to go to everyday. I had to live in an apartment where they said, and was subject to a curfew every night. I could not go on vacation or even go for a drive in the country without permission and an FBI agent assigned to follow me around so I would not disappear on them and hide. I cannot say it was the best deal I ever made, but it certainly was better than going to prison. I guess I am a lot like Frank Abagnale. I am to the electronic hacking what he was to forging checks back in the stone age.

5. The deal with the FBI had me working for them through the end of 2010. Over those years, I helped hunt down and convict a lot of prime time hackers. The hardest part about it was many of those people at the time were my friends when I was in the technological underground. A lot of people did not like the idea of me becoming a White Hat, also known as someone who works on the side of protecting assets. For a long time, hackers were people who were only interested in hacking to see how much money they could get. Then September 11, 2001, happened. Suddenly the focus of everything in the FBI changed. We started looking at hacking not just for the people who wanted to get rich, but for the people who wanted to do great harm to our country. I may be a criminal, but I would never do anything to destroy my country. Therefore, I happily moved to the cyber-terrorism unit inside the Bureau, and worked on identifying people and countries that could or would launch cyber-attacks against America.

6. Eventually at the end of 2010, I had worked off all my time with the FBI for the purposes of getting out from under the sentence for the Merrill Lynch hacking job. Once I was outside the FBI job/sentence, I had no more income. I decided not to go back down the path of a Black Hat. I thought my chances of getting caught again would be too great and I really did not want to do “real” prison time. I met and made friends with a lot of influential people while working on the FBI cases, which led me to the decision of starting

up a consulting business specifically for hacking related cases. I called it Gray Hat Consulting. Even though I was no longer a Black Hat, and have been working on the side of the government for a while, I could not consider myself a White Hat. Straddling between the two worlds led to the name idea of Gray Hat Consulting. Even I was surprised at just how fast my consulting business took off. At first, there were a few speaking engagements to local and state level law enforcement groups, and then several of the bigger businesses started hiring me to speak to their tech support staff and to evaluate their processes. Soon, I was back into networks and servers in a similar way as the old days, only without the destruction and felony charges from before.

7. Gray Hat Consulting was contracted by Ele Woods's defense attorneys on November 18, 2015, to look into the details of the prosecution's case. I do quite a bit of White Hat hacking, similar to what Professor Litt claims to be an expert in doing. I think Professor Litt is a joke and an "old time" kind of hacker. Professor Litt looks for an easy way of using young students or exploit computer programs versus actually looking at all the computer code, which is what I always do.

8. I have to say up front if Ele was the hacker who really ordered all the things they say, then Ele is the dumbest Black Hat out there. There are middle school kids with more and better abilities to cover up what they do. There are many rules about hacking. One of the most important rules is to NEVER USE YOUR OWN COMPUTER. How much more simple can it be to not use your own computer. Even with IP Address spoofing and forging MAC addresses, it always comes back to the government's ability to prove which computer was used. Here is a hint. Do not bet against the government. They got me. The government has an amazing amount of resources. Trust me, I know. Additionally, any "good" Black Hat is going to conduct the hack from a location with no ties to where the Black Hat normally operates. Best of all, there are free WiFi locations outside the normal operating range of the Black Hat. This way, the Black Hat does the hack, drives away from the location, and there is nothing to tie the Black Hat to the hack. A great example of this is Rivers Bread Company. Rivers offers free WiFi connection at all of their locations. They use great routers, so the signal carries a good distance. A Black Hat would drive to a Rivers location and sit in the parking lot to do the hack. The Black Hat never has to go into the physical location because there are store cameras or there is someone around to remember the person when the Feds come to investigate – and they will. The Black Hat can even go to a Rivers in the middle of the night after they are closed, because employees never bother turning the routers off. It is just too much trouble for the store to

bother turning the router on and off each day, so it leaves room for Black Hats to operate if they are up to no good. Nobody pays attention to a car sitting in a parking lot at night.

9. Ele Woods was not using another computer, but rather the one belonging to him/her, which was my first tip that this was not a Black Hat type of hack. Second, Ele was using the internet connection tied to the apartment Ele lived in, and thus breaking another cardinal rule of real hackers – NEVER USE YOUR OWN INTERNET CONNECTION. Third, all the information was there in the open including documentation of how the hack was accomplished, which is another rule of the Black Hats - NEVER WRITE ANYTHING DOWN OR PRINT ANYTHING OFF. Finally, Ele allegedly sent packages to the apartment without disguising who they were addressed to or where they were going, which is the last of the major rules – NEVER SEND THINGS TO YOURSELF. It is so easy to get a post office box in a fake name – it is not even funny. If someone is hacking and stealing, he or she should send the money or packages to a place where they can walk away from without getting caught if it is ever identified by the police. All those things combined lead me to believe that Ele Woods is the fall guy for someone else's bad acts.

10. Ele may have been engaged in White Hat hacking on behalf of Professor Litt. Shame on Professor Litt for getting an undergrad to do the dirty work while Professor Litt planned to take all the credit and the big payday. This intrusion was too systematic, detailed, and not stealthy enough to have been done by a "good" hacker. The hack was basically a textbook recipe for getting into a system, and did not possess the finesse or creativeness that a real Black Hat would have used. Not to mention, a Black Hat would have at least attempted to conceal the method of the breach in the event the Black Hat wanted to go back and steal more later – the exploit would not be shut down. A hacker would not worry with a small potatoes kind of hack like this. This sort of security intrusion is not worth the hassle versus the potential reward.

11. The IP and MAC addresses and the presence of some of the fraudulent items seized, led Agent Specter to jump to conclusions about the guilt of Ele Woods. The purchase information from Lilikoi's identified in the Order History from IP Address 22.231.113.64 has been marked as Exhibit #10. The computer was easily accessible by anyone who frequented the apartment, which I feel safe in saying was far more people than just Ele Woods and Micah Ross given the apartment was on a college campus. Agent Specter did not check Ross's computer for any evidence. Agent Specter did not conduct forensic checks to establish if IP Address Spoofing or MAC Address forging had occurred. If anything, Agent Specter should be thoroughly reprimanded for the sloppy investigation

tactics. This is certainly not something that should be expected of a SLED agent who previously worked for the FBI. All of this was noted in my report, which has been marked as Exhibit #9.

12. I am not a psychologist, but if I was trying to get rid of a rival, making them the fall guy would be an easy way to ruin that person. I think it would be far more likely that Micah Ross was jealous of Ele Woods's project with Professor Litt and stole the data right off Ele's desk to make the illicit purchases. Furthermore, framing Ele would embarrass Professor Litt who favored Ele over Micah, and get Ele out of the job pool upon graduation – one less person for Micah to compete with for professional employment. It is simple. Micah had the opportunity, the knowledge, and access to the information. And how coincidental is it that everything came to the apartment so Micah could enjoy it until inevitably the local law enforcement and SLED would catch up with them.

WITNESS ADDENDUM

I have reviewed this statement, and I have nothing of significance to add at this time. The material facts are true and correct.

Signed,

Quinn Bateman

Quinn Bateman

SIGNED AND SWORN to me before 8:00 a.m. on the day of this round of the High School Mock Trial Competition.

A.G. Molli

A.G. Molli, Notary Public
State of Hawaii
My Commission Expires: 12/15/17

1. My name is Ele Woods. I am 22 years old. I was born in Summerville, Hawaii, but I did not live there long enough to remember it at all. I grew up in a small town in Laupahoehoe on the Big Island called Ookala. I was in the Computer Engineering program at West Waiakea University (WWU). With everything that has happened over the past several months, the University asked me to take some time off. I suppose it was the most polite way of saying they threw me out for something Dr. Litt asked me to do! Since then and following the Indictments, I have been living back at home and spending all of my time working with my attorney to prepare my defense.

2. I knew from the time I was five that I wanted to work with computers. I can still remember my dad bringing home a Packard Bell computer with Windows 95. Looking back on it now, the computer was so pitiful with the slow modem and dial up internet access through America Online. Dial up internet service was painfully slow, but at the time I was mesmerized. From that experience, I knew my future career path was going to be in computers. I remember loving the sound of the modem until it connected with the internet and the simple online games my parents would let me play even at five years old. You can say I really grew up with technology, which might be why I was able to grasp technology at such a young age.

3. I think I was able to figure out before a lot of people our age that network security was going to be the big need in coming years. With every big business going online and stores selling everything imaginable online, it just made sense that people experienced in computer security would be needed to make computer networks safe. Everything we have seen in the last couple of years has reinforced the need for security to say the least. Between Target, Neiman Marcus, and Michaels losing millions of credit card data, not to mention the data breach at the Hawaii Department of Revenue, it was reinforced that network security was the right profession for me. There will always be bad people out there trying to take advantage of computer networks and people doing honest business. I saw my education and training as great tools to help prevent such things from happening.

4. I loved all my classes at WWU. After getting through a lot of the required general education classes and a couple of engineering classes, I was able to start working more on my computer engineering major during the spring semester of 2015. Classes started on August 15th. Every class had something new to learn. In particular, my classes

with Dr. Litt were my absolute favorite. Dr. Litt made a point to go beyond the theoretical discussions and look at how everything applied in the real world. The Systems Engineering class and the Professional Issues class were the last classes I took with Dr. Litt. I liked them the most because Dr. Litt used the Systems Engineering class to show real world application of building secure networks and data systems. Dr. Litt's Professional Issues class was really cool because it was all about ethics and how to operate ethically in the computer world. The moral of the Professional Issues class was kind of like Google's motto "Don't be Evil." It is a shame I did not get to finish the class. But then again, I am out because of Dr. Litt, so I do not know if I would take his/her classes again given my current situation.

5. I pretty well aced every computer engineering class I took at WWU. I even took quite a few of the optional courses to expand the knowledge base I would have to work with. All of the classes clicked for me, and I was always pushing most of my professors for more challenging things to do. But, I never had to push Dr. Litt. There was always an extra challenge or opportunity to do more with those classes – inside and outside of class. I did a lot of volunteering with Dr. Litt's research projects through the University. The volunteering work allowed me to see many projects that Dr. Litt and other instructors had. The volunteering kept me really busy and prevented me from going home on the weekends. Some of the projects were so cool! Some of the projects will later change how we use technology on a daily basis. Other projects dealt with home automation and the security behind it to make sure people could not hack our homes and turn home devices against us. The other side effect of the volunteering was that many professors started to hire me for random parts of their contract projects. Working on some of those projects put a little money in my pocket and put my name out in the real world – at least I thought it did. After finding out Dr. Litt never listed me on the contract with Lilikoi's, I wonder if anyone listed me on their projects either.

6. Micah Ross was my roommate at the on campus apartment in South Quad. An accurate diagram of our apartment 230 South Quad has been marked as Exhibit #7. It was a great apartment to be in, because from 230 South Quad to the Cannon building where my classes were was only a three minute walk. If I was running late I could run it in probably a minute and a half. Early on, I thought it was a good idea to have another computer engineering student as a roommate because we all have such weird study hours and lab times. Looking at it now, I do not think it was a good idea at all. We moved into the apartment the first week of May 2015, so we could both take advantage of the summer

semester classes. Micah was an okay student, but I do not think it came as easily to Micah as it did for me. It was probably tough seeing me excel while Micah muddled along and struggled to do well enough to get the grades needed for a good job after graduation. Micah would say snide things to me after we had been sharing the on campus apartment for a couple months. The comments made me feel bad, but it should not be my problem if I am better with computer systems than Micah. It started to make me mad, and eventually I tried to avoid Micah as much as I could.

7. On August 21, 2015, after the Professional Issues class, Dr. Litt asked me to stay after class. I figured it had to do with a research project I had been wrapping up for Dr. Litt's Hawaii Department of Motor Vehicles (SCDMV) Systems Improvement grant. I was clearly wrong on why I was asked to stay. Dr. Litt waited until everyone was out of the classroom and then shut the door. Dr. Litt revealed to me s/he had just acquired an incredibly cool contract with Lilikoi's. The contract was to do real world testing of Lilikoi's IT security systems. Dr. Litt offered me $2,250 in addition to the resume building experience I would gain. Because of the charges against me, I never got paid for proving the vulnerability in Lilikoi's secure financial transaction servers.

8. Testing of Lilikoi's security was to be done in a couple of different ways. Dr. Litt was traveling around the South east, and randomly testing the physical security of data processes in ten stores. To test the physical security of data in their stores, Dr. Litt was going into actual stores and looking around for computers and registers (which are computers now after all), which were left unlocked and unattended to see what could be pulled without being noticed. While at a Lilikoi's store, Dr. Litt was looking for unsecured Wi-Fi devices tied into the store networks, which could be a major security vulnerability.

9. The other part of Lilikoi's contract, which Dr. Litt asked me to do was to work on the e-commerce site of Lilikoi's. The e-commerce site is what you commonly know as an online store. The portion of the contract I was working on was to assess how much risk existed for customers to lose their data through a security breach of an online shopping experience, by attempting to create a breach and take data from Lilikoi's secure financial transaction servers. I thought it was an awesome opportunity to make a company safer and at the same time show off my skills and knowledge of network systems. This project was going to make my resume clearly stand out after graduation and everyone would want to hire me.

10. Dr. Litt swore me to secrecy and told me there would be a Non-Disclosure Agreement (NDA) for me to sign later. I never received an NDA for this project, but I have signed them for other projects I have worked on in the past. In the meantime, there was a pattern and process to the work I was going to be doing. The coolest part of this contract was to compromise Lilikoi's online store. The goal of this task was to gain access to sensitive data, specifically the credit card information, and then use five predetermined credit cards (all issued to Lilikoi's) to make various small online purchases to prove the breach. Once completed, I was to provide proof of the breach, and Dr. Litt would report back to the Director of Operations at Lilikoi's as to how the breach occurred, so security patches to the network could be made to eliminate the risk. It was definitely a big task, but one I was ready to tackle.

11. Because of being sworn to secrecy, I could not tell Micah about any part of the contract, but I am pretty sure Micah figured out that I secretly was working on something cool. From that point on, Micah seemed mad and was forever asking me what I was working on at the apartment and if I was going to head to the computer labs when s/he did. Micah and I used to go to the computer labs together at the same time. We went to the labs at the same time because we had a couple classes together and it was easier to go right after class. A copy of both of our class schedules has been marked as Exhibit #11. Once I started working on Dr. Litt's project, I decided to go to the computer labs at a different time from Micah to work in a little peace at the apartment without interruption while Micah was gone. In computer engineering, the computer labs are open 24 hours a day for students to come and go as they need. Leaving my laptop at the apartment while I was working on this project occasionally made me nervous because Micah was so nosy.

12. Ultimately, I was able to get into Lilikoi's online store and compromise the security on September 10, 2015. It revealed a lot of credit card information including the five specific cards I needed to prove the breach. I printed off probably 20 pages of credit card numbers with expiration dates. One thing I was not able to get was the CVV number found on the back of the credit cards. The reason I was not able to get those CVV numbers is because Lilikoi's did not use that additional security check. Because Lilikoi's did not require the CVV information, I could only use the compromised credit cards to make purchases on the Lilikoi's site. It did not matter to me that the credit cards could not be used at more secured sites, as the only thing I was instructed to do was to make purchases of less than $50 on each of Lilikoi's five pre-determined credit cards. Although I had permission to spend $50 on each of the cards, I felt that a ten dollar purchase on each

would be sufficient to prove the breach. I used the five credit card numbers to buy several packs of Wrigley's 5™ chewing gum – I really like chewing gum. I ordered three jumbo packs with each of the five designated credit cards and had the gum delivered to my apartment. Ordering chewing gum was also something that would fit easily in the mailbox outside our apartment door at South Quad. After ordering the chewing gum, I had to wait a couple days for the deliveries before being able to tell Dr. Litt about my success. I really wanted to have the gum in hand as proof of the security breach. I received the last package of gum at my apartment after Friday's classes, opened the boxes, tossed the packaging, and put everything in my backpack for class on Wednesday, September 23rd. After classes that day, I went to Dr. Litt's office, dropped the packs of gum on Dr. Litt's desk and said triumphantly: "This is courtesy of Lilikoi's." I think Dr. Litt was really impressed with me. We spent the next hour or so talking about how I accomplished the hack and about what Lilikoi's security system lacked. Once we concluded our conversation about all the security problems, Dr. Litt told me to make sure I secured all the information I retrieved from Lilikoi's system, as well as the processes I used to gain entry, and turn the documentation over as soon as I could. Prior to working on the project, I gave my IP and MAC addresses to Dr. Litt. I did that so if my breaching attempts were discovered by Lilikoi's, we would be able to prove it was me and not a random hacker really trying to do harm to their systems.

13. Right after I cracked into the Lilikoi's system, I noticed a few extra boxes around the apartment. I really did not think anything about it. Micah's parents were forever sending care packages. I mean we were juniors in college already. We both have September birthdays, and mine is on the 10th, but it still seemed crazy for Micah to get all those packages. Besides I did not care for the violent video games on the Xbox Micah played on the giant TV that must have been one of Micah's birthday presents. The only packages in the apartment I opened or paid any attention to were the ones with my name on them. The shipping labels seized by police in our apartment were marked as Exhibit #8, but only one of the shipping labels was from my orders.

14. A few days after some of the packages showed up, SLED agents and the University Police also showed up and raided our apartment on October 3, 2015. They seized my computer, and took a bunch of stuff out of the apartment. The copy of the warrant and the copy of the itemized seizure list were marked as Exhibit #5, and Exhibit #6 respectively were left in the apartment. The next day Agent Specter met me at my apartment, took me to the WWUPD, questioned me, and then arrested me. I found out after

my arrest that Micah told them all sorts of stuff about what I had been doing. Funny how Micah would know what I was working on when it was a secret and we did not talk about it at all. I did not even let Micah see my computer screen when I was working on the project for Dr. Litt. Agent Specter told me Micah provided information about me hacking and printing all kinds of credit card information and that I was using that information to buy things online. I never got the chance to prove my innocence and show the predetermined credit cards issued to Lilikoi's I was supposed to use and the chewing gum I ordered. Looking at it now, I should have locked up the printed pages of credit card information to keep them away from my roommate. Better yet, I should have kept my laptop with me at all times. And, I should have never chosen Micah as a roommate.

15. I know Micah saw the credit card information and figured out my secret project. Micah made the fraudulent purchases and had them shipped to our apartment. When the police caught on, Micah blamed me for it so I would get kicked out of school and go to jail while Micah would get off scot-free.

WITNESS ADDENDUM

I have reviewed this statement, and I have nothing of significance to add at this time. The material facts are true and correct.

Signed,

Ele Woods

Ele Woods

SIGNED AND SWORN to me before 8:00 a.m. on the day of this round of the High School Mock Trial Competition.

Michala Watson

Michala Watson, Notary Public
State of Hawaii
My Commission Expires: 4/3/19