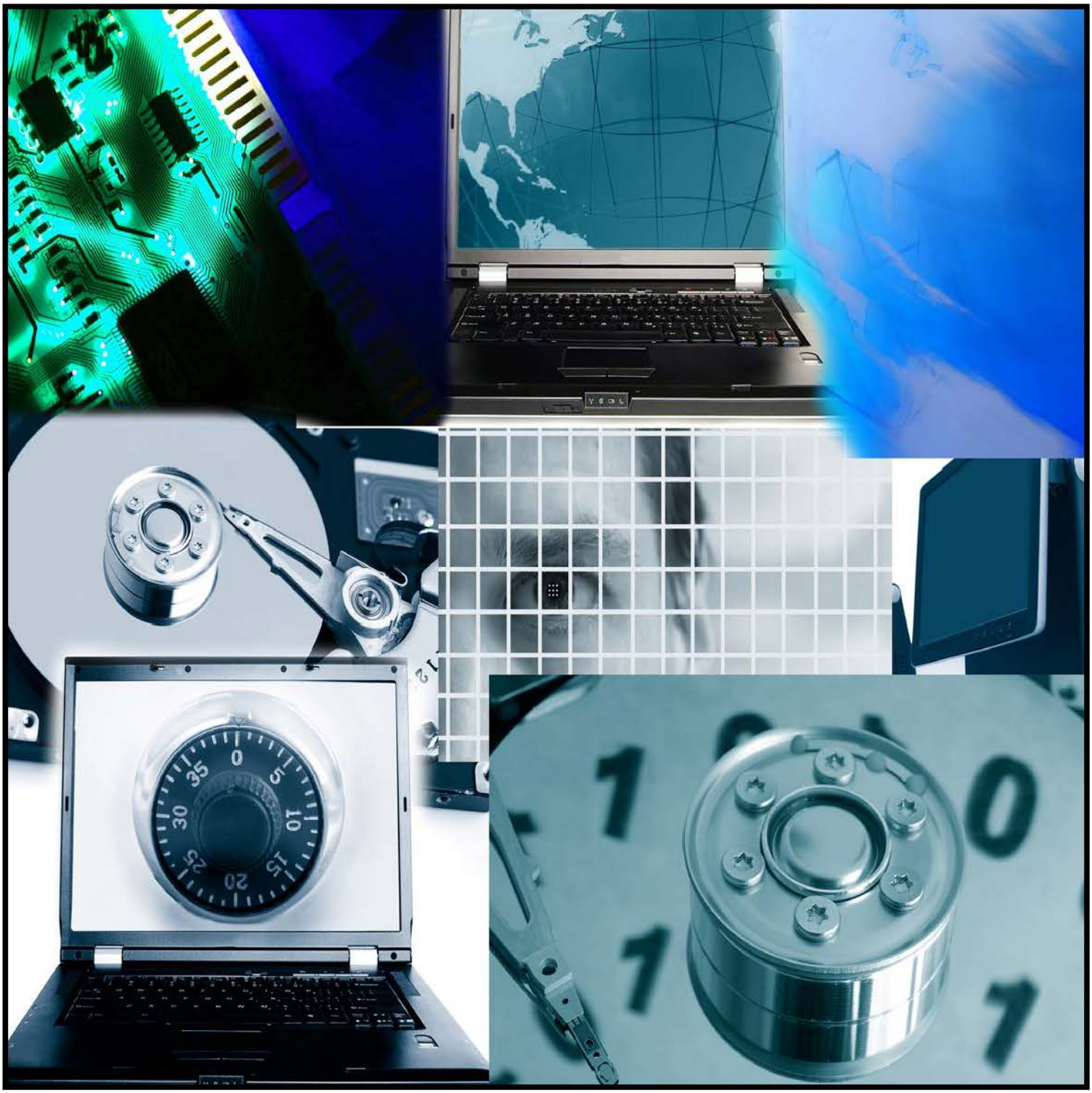
High Technology Crime In California – FY 09/10



Annual Report to the Governor and Legislature
Submitted by the High Technology Crime Advisory Committee

Table of Contents

Letter from Chairman of the High Technology Crime Advisory Committee 1

High Technology Crime – The Problem 2

High Technology Crime – The Solution.....5

High Technology Crime – The Future and Recommendations.....7

Task Force Profiles

- Northern California Computers Crimes Task Force (NC3TF).....8
- Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF).....14
- Rapid Enforcement Allied Computer Team (REACT).....21
- Southern California High Tech Task Force (SCHTTF) 25
- Computer and Technology Crime High-Tech Response Team (CATCH)..34

California Department of Justice – Advanced Training Center Activities.....36

California Attorney General – HTTAP Support.....40

California District Attorney's Association Activities.....41

California Penal Code Section 13848-13848.8 42

High Technology Advisory Committee By-Laws.....51

High Technology Advisory Committee Roster.....56

December 2010

Dear Governor Schwarzenegger, Senate President pro Tem Darrell Steinberg and Speaker of the Assembly John Pérez:

High technology crime and identity theft continue to pose major threats to California, its citizens, its industries, and its enterprises. The losses suffered by California on an annual basis reach into the billions of dollars. These losses represent *direct losses* suffered by individual victims and corporations and *indirect losses* resulting from lost wages, lost corporate profits, and lost tax revenues.

Since the inception of the High Technology Theft, Apprehension, and Prosecution (HTTAP) Program nearly twelve years ago, technology has continually evolved - from computers with floppy drives to home computers with terabyte hard drives. Pagers and PDAs have given way to cell phones and mobile devices with computer-like capabilities. Unfortunately, criminals have kept pace with technology, using it to find new ways or updating old ways to exploit California citizens and businesses.

There are five regional task forces that comprise the HTTAP Program. These task forces were established under Penal Code Section 13848 and receive oversight from the High Technology Crime Advisory Committee. These task forces receive support and training from the California Department of Justice and the California District Attorneys Association. The constantly changing nature of technology has been and remains a challenge for each individual task force and its affiliate agencies.

At the time of this writing, funding for these task forces for fiscal year 2010/11 is uncertain. The uncertainty of future funding has further challenged each task force and its affiliate agencies; with many forces being forced to delay critical training for investigators and prosecutors. Equipment purchases have been canceled or put on hold. Affiliate agencies are questioning their future affiliation with the task forces and the HTTAP Program. Without continued funding, law enforcement and prosecutorial agencies will be unable to meet the demands of changing technologies, as their expertise falls that of the criminals seeking to exploit Californians.

This report provides an overview of the HTTAP Program for fiscal year 2009/10. As you will see, the State invested just over $11.5 million for this program. While these funds allowed the task forces to investigate cases involving thousands of victims, losses amounted to more than $85 million. I urge you to read this report and give careful consideration to the recommendations. Your consideration and action will impact the safety of California citizens, California businesses, and the California economy.

Respectfully Submitted,
William E. Eyres
Chairman, High Technology Crime Advisory Committee
California Emergency Management Agency

The Status of High Technology Crime in California
The Problem

California continues to lead the nation in information technology (IT). According to the *Cyberstates 2010*[1] report, California is the leading state for high tech employment and also leads the nation in the net number of tech jobs created. The report also found that California was first in computer systems design and related services employment; first in internet and telecommunications services employment; first in research and development testing labs employment; and first in engineering services employment. Correspondingly, the citizens of California continue to expand their use of computers, the internet, and cell phones. Currently 93 percent of all residents say internet access is very important, and eight out of every ten Californians report using a computer at home, work, or school.[2] The use of mobile devices such as cell phones also continues to increase. Currently 84 percent of California residents use a cell phone. Of these users, 64 percent use their phone to send and receive text messages, and 30 percent use their phone to access the internet.

Unfortunately, this increase in technology has also brought about a corresponding increase in cyber crime. According to the *2009 Internet Crime Report,*[3] there was a 23 percent increase in the number of internet crime complaint submissions nationwide, with 336,655 complaints received in 2009. This however, is not a true representation of high technology crime today. Less than half of all cybercrime victims report their crime to the police or their financial institution.[4]

Cybercrime continues to be a problem in the corporate sector as well. According to the *2010 CyberSecurity Watch Survey,*[5] 60 percent of companies surveyed experienced a cybersecurity event during the prior 12 months despite increased budgets for IT security, corporate security, and physical security.

There are tremendous financial losses associated with cybercrime for the California economy, its businesses, and every citizen who becomes a victim of these crimes. According to the *CyberSecurity Watch Survey*, each corporate cybersecurity event

[1] Tech America Foundation: http://www.techamericafoundation.org/cyberstates
[2] Public Policy Institute of California: http://www.ppic.org/content/pubs/survey/S_609MBS.pdf
[3] Internet Crime Complaint Center: http://www.ic3.gov/media/annualreport/2009_ic3report.pdf
[4] Norton Cybercrime Report: The Human Impact: http://us.norton.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf
[5] 2010 CyberSecurity Watch: http://www.csoonline.com/documents/pdfs/2010CyberSecurityResults.pdf

results in an average monetary loss of $395,000. To the individual citizen who is a victim of cybercrime, it costs them an average of $334 and an average of four weeks to resolve the issue.

Individuals are using their computers and cell phones to access the internet in record numbers. However, these same individuals do not feel safe using these same tools. Nearly nine out of every ten adults thinks about cybercrime, and only three percent do not expect to become a victim of cybercrime.[6] Equally disturbing is the fact that nearly a third of all victims say their cybercrime issue was never resolved. According to the *Norton Cybercrime Report*, people "are being socially engineered to 'click here' and fall for cybercrime."

While internet crime is only a portion of the crimes investigated by the Task Forces, it makes up a significant portion of cybercrime as a whole. The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance. The mission of IC3 is to serve as a vehicle to receive, develop, and refer criminal complaints regarding cybercrime. As of November, 2010, the IC3 has logged over two million consumer complaints alleging online criminal activity. The IC3 compiles an extensive annual report[7] regarding internet crime. Data on internet crime is available on both a national level and a state level.

The data compiled by the IC3 indicates that in those cases where the victim was able to identify a suspect, the largest number of suspects resided in California. Additionally, California was the state with the highest number of victim complaints filed with the IC3. The table below is a breakdown on complaints received from victims in California during 2009.

Complaint Type	Percentage of Complaints
Non delivery of merchandise/payment	14.4%
FBI scams	14.0%
Identity theft	9.7%
Advance fee fraud	8.1%
Overpayment fraud	8.0%
Credit card fraud	7.2%
Miscellaneous consumer fraud	6.9%
SPAM	5.9%
Auction fraud	4.7%
Computer intrusion/hacking	4.4%

[6] Norton Cybercrime Report: The Human Impact: http://us.norton.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf

[7] Internet Crime Complaint Center: http://www.ic3.gov/default.aspx

During 2009, the IC3 received a total of 39,758 complaints from the state of California. **The complaints represented a loss to California victims that exceeded $92,400,000.** These losses represent a significant impact to California citizens and its economy as a whole. The highest dollar loss from a single complaint involved advance fee fraud and exceeded $9 million.

The table below is a breakdown on the dollar loss reported by California victims.

Monetary Loss	Percentage of Complaints
$.01 - $99.99	19.7%
$100.00 - $999.99	38.5%
$1,000.00 - $4,999.99	28.8%
$5,000.00 - $9,999.99	5.6%
Over $1,000.00	7.4%

The Status of High Technology Crime in California
The Solution

The California High Technology Crimes Task Force strategy was created in 1998 through Senate Bill 1734, to help combat computer-related crimes such as network intrusions, computer hacking, counterfeiting and piracy, theft of trade secrets, theft of high tech related equipment, and telecommunications fraud. This legislation established the High Technology Theft Apprehension and Prosecution (HTTAP) Program which is now managed through the California Emergency Management Agency (Cal EMA). The HTTAP Program includes five regional Task Forces covering 29 counties and encompassing a population of over 31 million. The program was expanded in 2001 to include an identity theft component.

The five regional Task Forces are:

- Northern California Computer Crimes Task Force (NC3TF)
- Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)
- Rapid Enforcement Allied Computer Team (REACT)
- Southern California High Tech Task Force (SCHTTF)
- Computer and Technology Crime High-Tech Response Team (CATCH)

Areas of Task Force coverage

The mission of the HTTAP Program is the investigation, apprehension, and prosecution of high technology crimes and to combat identity theft. High technology crimes (or cybercrimes) are generally defined as any type of illegal activity that makes use of the internet, a private or public network, or an in-house computer system. The directed groups of attack are the following three categories: personal, property, or government. Following are the components of cybercrime:

- Malware and malicious code
- Denial-of-service attacks
- Computer viruses
- Cyber stalking
- Theft of intellectual property
- Identity theft
- Network intrusions (hacking)
- Cyber terrorism
- Extortion
- Counterfeiting and piracy
- Email extortion
- Auction fraud
- Reshipping
- Phishing, pharming, spearing, and whaling

The HTTAP Task Forces partner with the private industry to help companies prevent, detect, and respond to computer-related crimes. The Task Force's personnel are highly trained professionals who also draw upon the expertise of private industry, academia, and government IT specialists to serve the corporate and individual citizens of California.

The statistics below represent the activities of the Task Force for the period of July 1, 2009 – June 30, 2010.

Cybercrime Investigations:						
	NC3TF	**SVHTCTF**	**REACT**	**SCHTTF**	**CATCH**	**Total**
Cases Investigated	42	554	111	76	61	844
Victims in Cases Investigated	1,147	650	119	130	14	2,060
Dollar Loss to Victims	$290,082	$29,678,709	$44,948,746	$703,000	$695,471	$76,316,008
Arrests	24	28	33	1	8	94
Cases Filed for Prosecution	3	124	22	3	8	160
Convictions	0	149	7	2	13	171
Forensic Examinations	30	493	83	398	166	1,170
Presentations Given	0	91	7	0	24	122

Identity Theft Investigations

	NC3TF	**SVHTCTF**	**REACT**	**SCHTTF**	**CATCH**	**Total**
Cases Investigated	35	180	114	90	49	468
Victims in Cases Investigated	181	29,946	380	111,690	77	142,274
Dollar Loss to Victims	$1,153,580	$1,344,820	$2,038,742	$6,595,173	$500,828	$11,633,143
Arrests	8	151	41	234	15	449
Cases Filed for Prosecution	0	365	21	130	13	529
Convictions	8	115	19	68	9	219
Forensic Examinations	0	9	65	0	0	74
Presentations Given	0	31	8	11	30	80

The funding provided by Cal EMA in support of this program is detailed below:

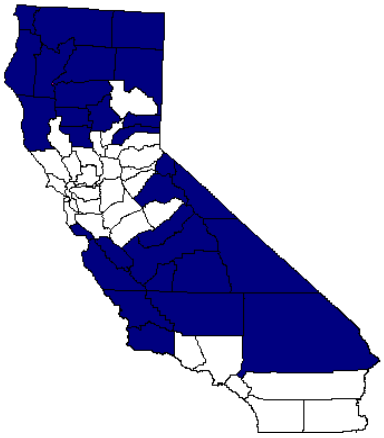
Task Force	**CalEMA Funding**	**Match Funding**	**Total Funding**
NC3TF	2,105,425	526,356	2,631,781
SVHTCTF	2,105,425	526,356	2,631,781
REACT	2,105,425	526,356	2,631,781
SCHTTF	2,105,425	526,356	2,631,781
CATCH	2,105,425	526,356	2,631,781
CDAA	208,324	52,096	260,420
DOJ ATC	425,160	0	425,160
DAG Support	372,348	93,087	465,435
Total	11,532,957	2,776,963	14,309,920

The HTTAP Program has been an innovative solution to fighting cybercrime in California.

The Status of High Technology Crime in California
The Future

Since the creation of the High Technology Theft, Apprehension, and Prosecution (HTTAP) Program twelve years ago, technology has changed tremendously. We have gone from slow computers with floppy drives to home computers with terabyte (or larger) hard drives. Pagers and PDAs have given way to handheld computers and cell phones with computer-like capabilities. While the direction technology will take in the future is somewhat uncertain, we do know that criminals will quickly adapt and develop new ways to victimize California's citizens. Criminals will take advantage of the new and ever-changing technologies to develop new ways to exploit the citizens and businesses in California.

It is vital that we as citizens, businesses, and governmental entities take a proactive role in protecting California from cybercrime. It is not only vital to every citizen in California, but to the overall economy of California.



Funding for the HTTAP Program has decreased over the years, and future funding for the task forces is uncertain. This report stated previously that the task forces collectively cover a 29-county region with a population of over 31 million. What this also means is there are an additional 29 counties not covered by any task force and over 7 million citizens that do not have access to a high tech crimes task force. On the map to the right, the highlighted areas represent counties that are not represented by any of the HTTAP Program task forces.

It is imperative that funding for the Task Forces be assured for the coming years. If funding is not continued, there will be an explosion of cybercrime in California. Investigators and prosecutors will not be kept abreast of changing technology and ever-evolving criminality. During fiscal year 2009/2010 the state of California made an $11.5 million investment in the future of California by funding the HTTAP Program. If this investment were continued or even increased, a step would be taken to ensure that California would be a safe and secure location for its citizens and businesses.

We recommend:

- Funding for the HTTAP programs be maintained, or even increased
- Funding be added to allow coverage of unrepresented counties
- Continuation of public awareness programs focused on cyber crimes

Northern California Computer Crimes Task Force (NC3TF)

Lead Agency: **Marin County District Attorney's Office**
The NC3TF is represented by the following six counties with a combined population of more than 2 million:

- Contra Costa
- Lake
- Marin
- Napa
- Solano
- Sonoma

Through a common memorandum of understanding, the NC3TF is comprised of participants from the following agencies:

- Contra Costa County District Attorney's Office
- Lake County District Attorney's office
- Marin County District Attorney's Office
- Napa County District Attorney's Office
- Rohnert Park Department of Public Safety
- Sonoma County District Attorney's office
- U.S. Secret Service
- Vallejo Police Department
- Walnut Creek Police Department

Case Profiles

Manufacturing Counterfeit Checks and California Driver Licenses

In December 2009, a subject was arrested by the Sonoma County Sheriff's Office for multiple counts of check fraud and identity theft after being arrested with 35 fraudulent checks and corresponding counterfeit California driver licenses. The Northern California Computer Crimes Task Force (NC3TF) assisted in the continuing investigation of that case. During that investigation, Brad Hesse of Castro Valley, CA, was identified as the possible ring leader of this multi-jurisdictional crime spree. Hesse was currently wanted in four different counties in California for identity theft-related charges.

From evidence obtained during the investigation, it was believed that Hesse was currently operating out of the Sacramento area. Additional suspects were cashing the

checks throughout the Bay Area and Central Valley. Surveillance efforts later revealed that Hesse was staying at the Hawthorne Suites hotel in Sacramento.

On June 25, 2010, the NC3TF served a search warrant on Hesse's hotel room and discovered evidence of a sophisticated and extensive check fraud, identity theft, and mail theft operation. Computers, photography, and printing equipment, as well as hundreds of thousands of dollars in prepared fraudulent State of California checks with corresponding counterfeit California driver licenses, were seized; however, Hesse remained outstanding.

On July 7, 2010, the NC3TF, with the assistance of Agents from the California Department of Justice, tracked Hesse to a motel in Stockton where it was discovered that he had rented three rooms. During a search of those rooms, four additional suspects were detained and additional computers, printers, fraudulent checks and counterfeit California driver licenses were seized. Hesse was arrested and booked into the San Joaquin County Jail. The other suspects were released pending further investigation.

"Adobe Systems Incorporated is very appreciative of the work that NC3TF does in helping us fight software piracy. The illegal production and sale of counterfeit software is especially troubling to us, as it victimizes both Adobe Systems and the consumer. The cases that NC3TF takes on gets those illegal producers and sellers off the street. The approach that NC3TF takes in accomplishing this is innovative and efficient. With Adobe Systems losing hundreds of millions of dollars annually to software piracy, we devote significant resources each year to fighting this problem. We are very pleased to partner with NC3TF in combating software piracy."

Chris Stickle
Enforcement Manager, Anti-Piracy
Adobe Systems Incorporated

From preliminary searches of the seized computers, the personal identifying information of thousands of victims has been identified. The NC3TF is continuing the investigation into the additional suspects.

The NC3TF has been accepting for investigation, additional counterfeit check cases from local agencies which appear to be related. The ring targeted Wal-Mart and Safeway stores for cashing the "payroll" type checks. The NC3TF is working with the Asset Protection Departments of Wal-Mart and Safeway. Wal-Mart has been tracking this ring for the last year. The suspected loss to Wal-Mart alone is approximately $1.2 million.

To date the NC3TF had linked six additional suspects to this ring. The NC3TF is working with the State Attorney General's Office for prosecution.

Gas Pump Skimmers

In February, 2010, the NC3TF met with law enforcement agencies after multiple agencies from Solano and Contra Costa counties reported a dramatic increase in identity theft cases. It was discovered that all the victims frequented common gas stations. During the investigation, a skimming device was located on a gas pump in the city of Benicia. The NC3TF became the central information hub to gather and disseminate information between the agencies regarding these cases.

Days later, the Martinez Police Department was notified that an employee at a 7-11 Store/Gas Station located a skimming device on one of their gas pumps. Martinez Police Detectives removed the device and replaced it with a similar looking device.

The devices were inside the gas pumps' housing and were not visible. The pumps' housings are locked, but many use a common key. The suspects needed to have one of those keys to open the housing to plant and retrieve the device.

Martinez Police contacted the NC3TF for personnel support in conducting surveillance on the pump in an attempt to apprehend the suspects when they returned to retrieve the device. 24-hour surveillance was established on the gas pump. In the early morning hours of February 26, 2010, two suspects were arrested when they accessed the mock device. Both suspects were Armenian Nationals and have been linked to an Armenian gang from Southern California.

The two suspects were booked into the Contra Costa County jail. A search of the suspect vehicle revealed two additional skimmers and two GPS navigation units. On the GPS units, there were recent searches for 7-11 and Arco Gas Stations in the following cities: Martinez; Stockton, West Sacramento, Sacramento, Davis; Dixon, San Leandro, Walnut Creek, Danville, Hayward, San Mateo, Elk Grove, Lodi, Dublin, Livermore, San Ramon, Carmichael, Citrus Heights, Fairfield, Castro Valley, and Concord. The devices contained credit card and ATM card account information for over 200 victims.

The NC3TF and Martinez Police Detectives physically checked all gas pumps at the stations identified in the GPS units and recovered an additional eight devices. A hotel key was also found in the vehicle which linked those suspects to additional suspects who had been staying at that hotel. Arrest warrants have been issued for two other suspects.

Through Automated Teller Machine (ATM) surveillance photographs, a third suspect was identified. The NC3TF obtained a warrant for the third suspect's arrest and a search warrant for his residence in Los Angeles. With the assistance of the SCHTTF, the warrant was served and the suspect arrested. Additional evidence linking the third suspect to the crime ring was found.

The initial case was filed by the Contra Costa County District Attorney's Office but has since been transferred to Deputy Attorney General Keith Lyon. The NC3TF is continuing to work with DAG Lyon and the Martinez Police Department on this case.

Software Piracy

On May, 6, 2010, the NC3TF received a complaint from the Autodesk License Compliance Division of a person advertising the sale of Autodesk software on Craigslist. The NC3TF conducted an undercover purchase of Autodesk software in Marin County.

During the purchase of the software, the suspect confirmed that the software was not a licensed copy. After the purchase was complete, the suspect was arrested and booked into the Marin County jail.

A search warrant was issued and served on his residence in San Jose where additional evidence was obtained.

Network Intrusion

The NC3TF received a complaint from a Marin County-based organic skin care company, Juice beauty.com. The company had been working with a web site designer from the Southern California area. The skin care company became increasingly dissatisfied with the designer and ultimately terminated the working relationship. To retaliate, the designer, while unauthorized to do so, logged in to the company's website, assumed Administrator status, and locked the company out of their own website. Additionally, he disabled part of the company's shopping cart, therefore

"On behalf of Autodesk, Inc. a computer software manufacturer and member of the steering committee for the Northern California Computer Crimes Task Force (NC3TF), I would like to send a note of thanks and appreciation to the Task Force.

Software piracy and distribution of counterfeit products continues to be a serious problem for software manufacturers. It impacts our financial success and ability to grow our business and remain competitive.

Software development involves a tremendous collaborative effort from development engineers, designers, programmers, artists, and others. When software is copied and sold illegally, it impacts our revenues. Additionally, distribution of our software through a channel of resellers authorized by Autodesk, creates jobs and contributes to the economic success of large and small businesses throughout California. The proliferation of online sales, auctions, and sites such as Craigslist create a marketplace for distribution of illegally copied or counterfeit software.

NC3TF has taken an active role in pursuing, investigating and prosecuting individuals that have copied and sold our software, in violation of both California and federal copyright and trademark laws.

Criminal remedies are the most effective deterrent we have to stop this illegal activity. Autodesk continues to support the efforts of the Northern California Computer Crimes Task Force and are grateful for the time and expertise needed to enforce the statues and laws related to intellectual property rights holders."

Evie LaHaie, Sr. Litigation and License Paralegal
Autodesk, Inc.

halting their ability to receive sales orders.

The web site designer then extorted thousands of dollars from the company by agreeing to allow the company access to their own web page only after the designer was paid money to which he was not entitled. Ultimately the company paid to obtain the passwords and regain control of their web site.

After an investigation by the NC3TF, an arrest warrant was issued by the Marin County Superior Court for the arrest of the web site designer for violation of California Penal Code Section 502 (c) (1).

On August 26, 2010, the NC3TF, with the assistance of the Southern California High Tech Task Force served a search warrant on the suspect's home for additional evidence. The suspect was arrested and booked at the Los Angeles County Jail. The suspect will be prosecuted by the Marin County District Attorney's Office.

Software Piracy

On June 2, 2010, the NC3TF received a complaint from Adobe Systems Anti-Piracy Enforcement Division of a person advertising the sale of Adobe Systems software on Craigslist. The NC3TF completed two undercover purchases of Adobe software from a Sonoma County man. The software was confirmed to be unauthorized copies.

After the second purchase, the suspect was arrested and booked into the Sonoma County jail. A search warrant was issued and served on his residence where additional evidence was obtained.

Identity Theft

On May 13, 2010, a Marin County Attorney, Mohamad Salem, reported to the Marin County Sheriff's Office that he was the victim of identity theft. Salem had been contacted by numerous attorneys from outside of Marin County regarding work Salem allegedly performed. Salem was not familiar with any of those cases. The victim, through his own investigation, found the website: canwinforeclosure.com, was advertising legal help with foreclosures and was using the victim's name and State Bar number. The Marin County Sheriff's Office referred the case to the NC3TF for investigation.

With the assistance of the attorneys who had contacted Salem, the NC3TF identified the suspect, Nicolas Moscouplos of Sacramento, California. A search warrant served on Moscouplos' Sacramento office and home, resulted in the identification of at least 12 victim clients. Moscouplos was preying on individuals who were nearing foreclosure of their homes. Moscouplos posed as Mohamed Salem, Attorney at Law, specializing in Foreclosure Law.

Moscouplos was arrested and booked for False Personation of Another, and Identity Theft.

As the investigation continues, additional victims have been identified. To date 15 victims have been identified with a combined loss of over $34,000.00.

Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)

Lead Agency: **Sacramento County Sheriff's Department**
SVHTCTF is represented by the following thirteen counties with a combined population of more than 3 million:

- Amador
- Calaveras
- El Dorado
- Mariposa
- Merced
- Placer
- Plumas
- Sacramento
- San Joaquin
- Stanislaus
- Sutter
- Yolo
- Yuba

Through a common memorandum of understanding, SVHTCTF is comprised of participants from the following agencies:

- Amador County Sheriff's Department
- Calaveras County Sheriff's Department
- Calaveras County District Attorney's office
- California Attorney General
- California Department of Insurance
- California Department of Justice
- California Highway Patrol
- Ceres Police Department
- Citrus Heights Police Department
- Davis Police Department
- El Dorado County Sheriff's Department
- Elk Grove Police Department
- Escalon Police Department
- Fairfield Police Department
- Federal Bureau of Investigation
- Folsom Police Department
- Galt Police Department
- Ione Police Department
- Jackson Police Department
- Livingston Police Department
- Lodi Police Department
- Manteca Police Department
- Marysville Police Department
- Mariposa County Sheriff's Department
- Merced Police Department
- Merced County Sheriff's Department
- Modesto Police Department
- Nevada County Sheriff's Department
- Placer County District Attorney's Office
- Placer County Sheriff's Department
- Plumas County Sheriff's Department
- Ripon Police Department
- Rocklin Police Department
- Roseville Police Department
- Sacramento County Department of Human Assistance
- Sacramento County Probation Department
- Sacramento County District Attorney's Office
- Sacramento Police Department
- Sutter County Sheriff's Department
- Tracy Police Department
- Turlock Police Department
- Twin Rivers Police Department
- U.S. Postal Inspection Service
- U.S. Secret Service
- University of California, Davis, Police Department
- USDA Forest Service
- Vacaville Police Department
- Yolo County Sheriff's Department
- Yolo County District Attorney's Office

"As you know, I can't thank your law enforcement agency and the California Highway Patrol enough or enough times in tracking down and prosecuting the people who were running a nationwide identity theft ring from Sacramento. I can't believe how fast everything got done once you were contacted by Christopher McClure from the Virginia State Police. If ever a case showed the need for multi-jurisdictional la wenforcement and how it should work, it was this case."

Senator Richard L. Saslaw
Majority Leader
Senate of Virginia

Case Profiles:

Software Piracy

Detectives assisted the Sacramento Cyber Squad unit with a search warrant. The suspect had been selling counterfeit copies of Rosetta Stone, Microsoft, and Adobe software via the internet. The search yielded two computers; one of which contained the counterfeit software files from which the suspect had been making illegal copies for sale. A desktop computer, blank CD-Rs, paper sleeves, and shipping labels were also recovered. In addition, 75 U.S. Postal Service delivery confirmation receipts were recovered from the target location as well. The suspect was not home during the service of the warrant; however, he was located at his place of employment. The suspect gave a full confession and agreed to assist federal agents with further investigation of this case. The suspect will be arrested after an indictment is issued. This case will be prosecuted in the federal system.

Identity Theft

The Hi Tech Crimes Task Force received information from Virginia State Police regarding the identity theft of Senate Majority Leader Richard Saslaw. A Sacramento address was identified as receiving mail and credit cards in Saslaw's name. A search warrant was issued, and all four suspects were identified. The victim's credit card was used at Fruitridge Health and Wellness to purchase medicinal marijuana. The card was also used at Twisted, Johnny Rockets, Sprint, Denny's, US Search and MacDonalds. The suspect was arrested at time of the search for an outstanding no bail warrant.

"With cyber crooks getting more and more sophisticated, the Sacramento Valley Hi-Tech Crimes Task Force does a tremendous job tracking down these dangerous criminals. Prevention plays an important role in stopping cyber crime. I've worked closely with the Task Force to provide my constituents with the information they need to protect themselves from becoming a victim."

Senator Dave Cogdill, R-Modesto
Vice Chair, Senate Public Safety Committee

Music/Movie Piracy

Detectives investigated a large-scale piracy case involving four retail stores in the greater Sacramento area. The suspect is the owner of four retail stores that specialize in DVD/CD rentals that cater to the Russian community. Three search warrants were

served over a four-day period. Eighty-seven thousand DVDs and CDs were recovered with an estimated value of $1.3 million. Investigators also discovered the suspect was defrauding his customers by overcharging their credit cards that were left on file. This case is currently being prosecuted in the federal system. The Task Force was assisted by members from the following agencies, Immigration and Customs Enforcement, Rancho Cordova Police, Sacramento County Probation, Department of Justice, West Sacramento Police, and California Highway Patrol.

Identity Theft

An untagged suitcase was returned to baggage claim at Sacramento International Airport. Airline personnel checked it for owner information and found an identification card, 25 credit cards, and a card reader/writer. The airline personnel then became suspicious and turned the suitcase over to the Sheriff's Department Identity Theft unit. The credit cards were suspected to be counterfeit when the telephone numbers on the backs of the credit cards did not connect with the banks on the face of the credit cards. Investigation by identity theft detectives revealed the credit cards and identification were counterfeit, and fraud transactions had been made with the credit card account numbers. A possible suspect was identified on surveillance video, and a search warrant was obtained for his residence.

Identity Theft

In February 2010, detectives located and arrested Mia Garza at her residence in Elk Grove. Garza had a felony PC 530.5(a) warrant for her arrest. Garza is on searchable probation out of Contra Costa County for an identity theft-related conviction. Garza was wearing an ankle bracelet monitoring device on her arm when arrested. Further investigation revealed Garza was committing additional identity theft crimes while on monitored probation. Garza completed her apartment rental application identifying herself with a name and SSN that legitimately belongs to another victim.

A search of Garza's apartment produced more than four credit cards in other person's names, multiple counterfeit California

"As criminal elements began to victimize our customers and our stores, Walmart seeks out assistance from our Law Enforcement partners to help ensure that our customers are protected and that these criminal elements are brought to justice. The California High Tech Crimes Task Forces have been an integral part of our success with these matters and we fully support their operations and applaud their passion in seeking justice on behalf of our customers and company alike. Without the assistance of the California High Tech Crimes Task Forces many of these successes would not have been possible. Their work, dedication, and cooperation with private sector retailers has led to numerous successful arrests and convictions, numerous merchandise and financial recoveries, and ultimately helped protect the citizens of California".

Mark McClain, Director
Asset Protection Investigations
Walmart Stores, Inc.

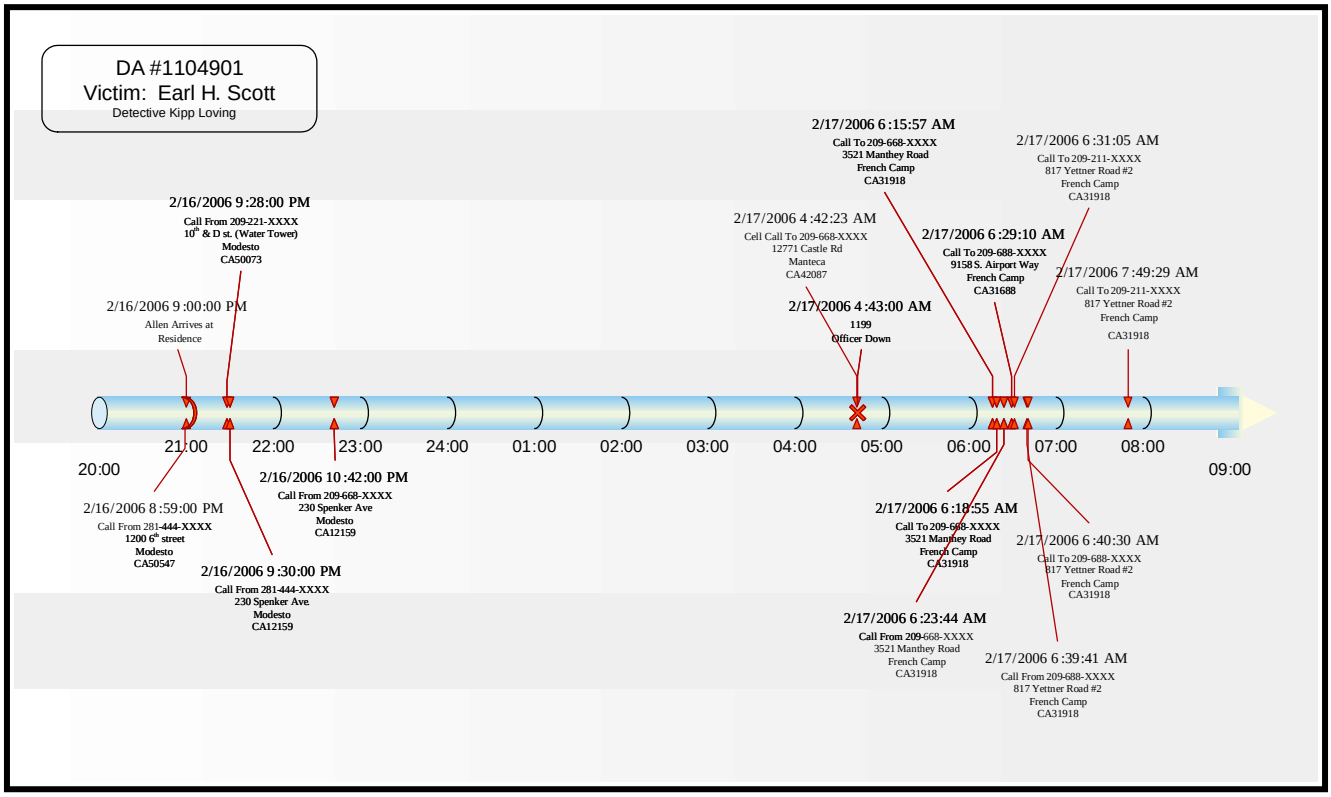
driver licenses, materials to manufacture counterfeit identifications, and counterfeit credit cards. A forensic exam of Garza's laptop revealed a file containing the personal identifying information of over 29,500 Kaiser employees. Approximately 400 of the employees have been victims of identity theft. Garza stole the file during her short employment with the Northern California Kaiser Employee labor union.

A search of Garza's storage unit produced thousands of dollars worth of stolen property and additional evidence of identity theft. Detectives also recovered an expensive puppy that was purchased online by Garza using a fraudulently-obtained credit card number.

Garza has identity theft cases pending in several counties as well as a federal case being pursued by U.S. Postal Inspection. Garza is currently being held in the Contra Costa jail. Garza has two $1,000,000 identity theft warrants for her arrest in Sacramento County. The Deputy District Attorney assigned to the Sacramento Valley Hi-Tech Task Force is handling the prosecution in Sacramento.

Cell Phone and Computer Forensics

Cell tower tracking data was used during the investigation of the homicide of CHP Officer Earl Scott. The chart below is a timeline of the suspect's movements based on the tracking data from his cell phone. The gun used during the homicide was never recovered; however, gun shot residue was found on the suspect's cell phone. The suspect pled guilty.



The timeline shows the suspect in Modesto at 10:42 p.m. At 4:42 a.m., the suspect is pulled over by Officer Scott. The “officer down” call is received at 4:43 a.m. Various calls are placed by the suspect over the next two hours as he goes to the homes of friends in Stockton to dump his car and change clothes. The suspect later admitted he had a gun and drugs in the car and did not want to go back to prison.

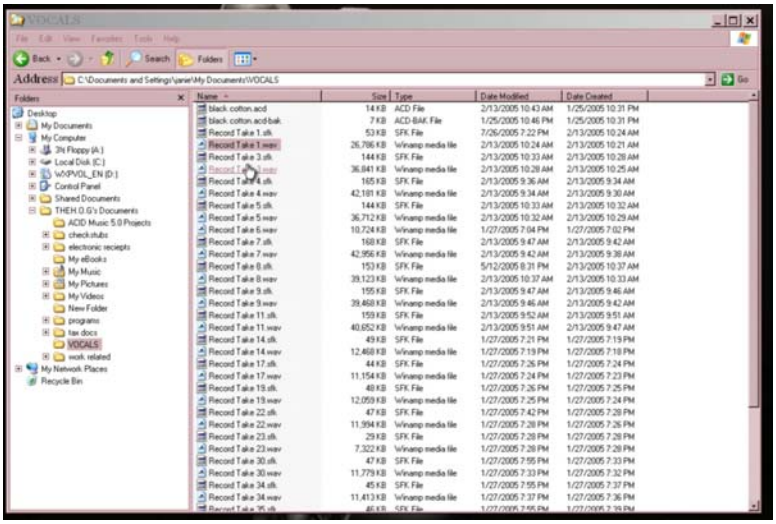
TPD 06-1994 Scott

The image on the left is a text message from one of the suspect’s friends. The message was sent shortly after the suspect left the friend’s house.

This is a photo of the gun presumed to be used during the homicide. It was found on the defendant’s computer.

This is a screen capture of the recordings made by the defendant from his computer.

Below are some of the lyrics to the recordings also found on the defendant’s computer.



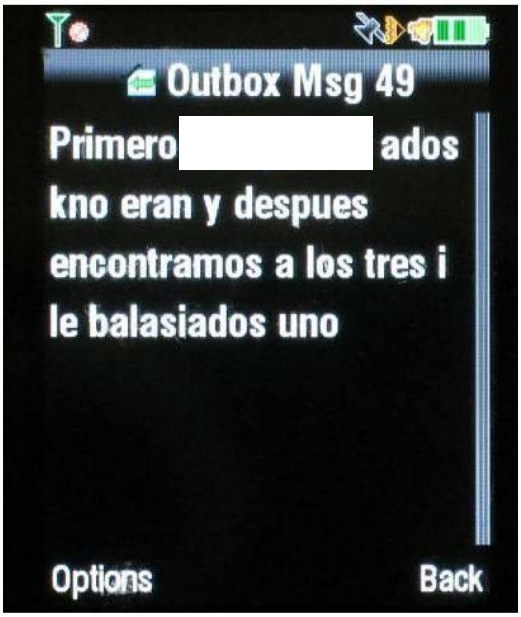
Record Take 3.wav "Oh, [redacted] We got a cop killer song ya'll. Let's kill all these mother [redacted] Yeah."

Record Take 1.wav "This is for all them dirty cops. This a cop killer song. We hadn't had one in a while ya'll. You know we need one…..grab your pistols, ride with them mother [redacted]…listen to what I'm telling you cause this [redacted] can be done……"

Record Take 8.wav "Yeah. This is a dirty cop song ya'll. I haven't heard a good cop killin' song in a while. It ain't like the thought ain't on our head or nothin'….."

Arson/attempted homicide investigation:

The message on the right was taken from a victim's iPhone as part of an arson investigation. The victim's husband attempted to burn down her home but was unsuccessful.



This text message was from a phone seized off of a suspect shortly after a homicide. The date/time stamp for the message indicates it was sent six minutes after the victim was killed in a drive-by shooting.

The translation of the message is:

"First we f#$%ed up two but it was not them and later we found the three and we shot one"

"I am writing you today to offer you my personal and professional endorsement of the Sacramento Valley Hi-Tech Crimes Task Force.

Identity theft is a growing problem in our society, and its ramifications are immense - both for the people whose identities are stolen, and for the people and companies defrauded as a result of theses thefts. We at SIRAS see these crimes occur every day, as our technology helps participating retailers by registering products at the point of sale and tracking them, helping to prevent and identify fraud and other crimes.

Because of the consequences of identity theft, and understanding that it will take the joint efforts of public agencies and private industry to effectively fight these crimes, SIRAS developed its Product Information database to help identify products that may have been stolen, and made the decision to provide law enforcement agencies access to it at no charge.

We are fortunate to have worked with Detective Sean Smith and the Sacramento Valley Hi-Tech Crimes Task Force, and we have seen, first hand, how the combined and coordinated efforts of these 40+ agencies have helped fight crime on the Sacramento area. We've also had the pleasure of working with Detective Smith, who has made himself available to the retail trade media to inform retailers of the ways they can help combat identify theft and the retail crimes that result.

With budgets being leaner than ever, and with technology making the perpetrators of these crimes harder to track down, we need more coordinated efforts like those by the members of the Sacramento Valley Hi-Tech Crimes Task Force. And on behalf of SIRAS, I encourage you to continue funding this valuable group. It is a true asset in the fight against identity theft and the resulting crimes."

Peter Junger, President
Siras

Rapid Enforcement Allied Computer Team (REACT)

Lead Agency: **Santa Clara County District Attorney's Office**
REACT is represented by the following four counties with a combined population of more than 5 million:

- Alameda
- Santa Clara
- San Francisco
- San Mateo

Through a common memorandum of understanding, REACT is comprised of participants from the following agencies:

- Alameda County District Attorney's Office
- Atherton Police Department
- California Department of Motor Vehicles
- California Highway Patrol
- California Attorney General
- Federal Bureau of Investigation
- Fremont Police Department
- Millbrae Police Department
- Mountain View Police Department
- Pacifica Police Department
- San Francisco County District Attorney's Office
- San Jose Police Department
- San Jose State Parole
- San Mateo County District Attorney's office
- San Mateo County Sheriff's Office
- Santa Clara County District Attorney's Office
- Santa Clara County Sheriff's Office
- U.S. Immigration and Customs Enforcement
- U.S. Postal Inspection Service
- U.S. Secret Service

Case Profiles:

Profile #1
A REACT Task Force Agent received a case in November 2009 involving the suspected internal theft of computer peripherals from Cisco Systems. Cisco Investigators observed, during an audit, that a local electronics parts reseller was checking the warranty status of peripherals listed as internal Cisco assets. The criminal investigation revealed that over the course of several years the suspect, a Cisco employee, stole internal assets from Cisco and sold them to a local reseller. Cisco initially estimated their loss at approximately $800,000.

The investigation revealed the loss was far greater than Cisco estimated. This was confirmed in statements provided by the suspect after his arrest. The suspect admitted he used the gains from his criminal activity to build a multi-million dollar home in the Fremont foothills. The suspect was ordered to sell the home and pay restitution in the amount of $2 million. As part of the negotiated settlement, the suspect provided a complete statement to REACT and Cisco investigators. The suspect provided details on how he was able to conceal his criminal behavior over the course of several years. Cisco was able to use this information to strengthen their internal controls.

Profile #2

In October 2009 REACT Investigators received a call from Redwood City asking for urgent assistance. Investigators in Redwood City were informed that an unknown person posted an ominous threat against a school on a web site forum. Investigators confirmed the threat had been posted and believed it could be credible. Because of the escalating acts of violence at schools around the nation, Redwood City asked REACT to assist them in attempting to identify the person responsible for posting the threat.

"The REACT task force has been an invaluable asset to local law enforcement agencies since 1997. Without REACT, many major fraud and identity theft cases would not be investigated due to lack of resources and expertise at the local level. It has become the go-to agency for high technology companies and law enforcement in the Silicon Valley.

Law enforcement must keep pace with today's sophisticated criminals who utilize the newest technology to steal from business and our citizens. Ensuring a stable funding source to continue the High Tech Task Forces in California is essential to public safety."

Dolores Carr
District Attorney, Santa Clara County

REACT Investigators executed an exigent request for information requesting subscriber records and IP address identification. REACT Investigator were able to trace the threat to a 15 year-old boy in Rocky Mount North Carolina. REACT Investigators contacted the Rocky Mount Police Department and provided them with the information they had received up to that point. Investigators assisted the local agency in preparing a search warrant for the suspect's residence. A search of the residence turned up drawings depicting explosives, but no destructive devices. The suspect was detained for making a false report of a destructive device and was later released to the custody of his parent pending a juvenile hearing.

"REACT is unique in nature as it maintains the knowledgeable personnel and expertise to go after criminals who engage in organized high tech crimes. Smaller agencies turn to REACT for assistance as they are often reluctant and/or unable to allocate the needed resources to investigate and successfully prosecute these cases."

Sheriff Greg Munks
San Mateo County Sheriff's Office

This is just one of many examples where the specialized experience and knowledge of REACT Investigators has been instrumental in assisting local agencies with their criminal investigations. In this case REACT investigators, working through established contacts, were able to identify the suspect in this case in just a matter of hours.

Profile #3

In August 2010 REACT received a case referral from investigators at Safeway Stores Inc. Safeway investigators received an anonymous tip that a Safeway customer was using fraudulent credit cards to purchase gift cards at numerous Safeway stores around the San Francisco Bay area. REACT Investigators, working closely with Safeway, identified the suspect and were also able to identify a specific profile of criminal behavior. Using this profile, Safeway was able to link the suspect to hundreds of fraudulent transactions in California, Washington and Nevada with an estimated loss of over $500,000.

"As agencies throughout the state are forced to downsize they no longer have the sworn staff to conduct traditional criminal investigations. More and more agencies are focusing on crimes against persons, often at the expense of property crime investigations. REACT has been able to adopt many High Technology and Identity theft investigations that would have other wise been closed at the local level."

Chief Peter Oliver
Bureau of Investigations
Santa Clara County
District Attorney's Office

REACT Investigators conducted surveillance and witnessed the suspect making fraudulent purchases at several Safeway stores. The investigation determined the suspect was employed as a desk agent for a major airline at the San Jose Airport. She was obtaining credit card information while processing payments for business travelers.

The suspect would re-encode credit cards with the information stolen from the unsuspecting travelers and use the fraudulent cards to purchase gift cards at Safeway. In a fairly complex scheme to avoid detection, the suspect would exchange the gift cards for higher denomination gift cards, typically $100 to $1,000. The suspect would then use the new gift cards to purchase high-end electronic and computer products. These products were then sold on eBay.

REACT Investigators also discovered that the suspect, in concert with other(s), was conducting shill bidding on eBay. The purpose of the shill bidding was to drive up the purchase price of the item being sold.

REACT Investigators determined the suspect has been conducting fraudulent credit card transactions every day for at least the last several years, possibly since 2001. The known loss to date is $500,000. She is suspected of being responsible for losses well over $1 million.

As part of their investigation, REACT Investigators determined that a report of fraudulent credit card activity involving the suspect was referred to the United States Secret Service in 2001. Because the case referral did not meet the dollar loss threshold to justify federal investigation the case referral was not pursued. This case is an excellent example of the void filled by the High Technology Task Forces in California. The Task Forces are perfectly positioned to handle those cases that would strain the

investigative resources of local agencies yet are not big enough to meet the high federal thresholds.

Southern California High Tech Task Force (SCHTTF)

Lead Agency: **Los Angeles County Sheriff's Department**
SCHTTF is represented by the following three counties with a combined population of more than 14 million:

- Los Angeles
- Orange
- Ventura

Through a common memorandum of understanding, the SCHTTF is comprised of participants from the following agencies:

- Beverly Hills Police Department
- California Department of Motor Vehicles
- Federal Bureau of Investigation
- Glendale Police Department
- Los Angeles County Department of Consumer Affairs
- Los Angeles County District Attorney's Office
- Los Angeles County Probation Department
- Los Angeles County Sheriff's Department
- Orange County Sheriff's Department
- Oxnard Police Department
- Santa Monica Police Department
- Simi Valley Police Department
- U.S. Department of Homeland Security-Immigration & Customs Enforcement
- U.S. Postal Inspection Service
- U.S. Secret Service
- Ventura County District Attorney's office
- Ventura County Sheriff's Department

Case Profiles:

JukeBox Investigation
This investigation was introduced to the Task Force by representatives of the recording industry and involved a suspect company named Sansel Enterprises. Sansel Enterprises rents jukebox machines to a number of restaurants catering primarily to Hispanic communities in Orange, San Bernardino, and Ventura Counties. The machines are modified with a hard drive system containing copies of music and music videos without the expressed consent of the artist. The music is sold to a listening audience for a profit every time a music selection is made and played. A federal search

warrant was served at a number of locations and hundreds of these machines were seized from restaurants. The search warrant also included the primary business. The exact monetary loss has not been determined. Unfortunately, the recent 9th Circuit Court decision concerning forensics examinations has impacted the federal government's ability to further prosecution in those cases involving forensics examination. As a direct result of this decision, this investigation has been stalled.

Hotel Spyware

High Tech investigators were requested by a major credit card bureau to assist hotel management in the city of Calabasas with an electronic fraud. Investigators determined that an unidentified suspect installed "spyware" onto the hotel's business center computer used by hotel guests. A forensic investigation identified a large number of hotel patrons who were being victimized in an elaborate scheme to steal identities to commit fraud. Within days, additional victim hotels, victim card holders, and the suspect were identified. The suspect was apprehended following approximately 19 hours of surveillance. Search warrants were served on his residence. Several computer systems and evidence of the identity thefts and frauds were seized by investigators.

Forensic Evidence

High Tech investigators played a key roll in the prosecution of two suspects involved in a gang-related attempted murder case. Forensic evidence extracted from the suspect's cell phones revealed text messages between the two suspects discussing an alibi along with numerous incriminating cell phone photos of several gang members. The Los Angeles County District Attorney's Hard Core Gang Unit prosecuted this case. Both suspects were convicted. One suspect received a 75-year state prison sentence. The other suspect received an 80-year state prison sentence. Both suspects are in their mid 20's. The victim is a 16-year-old boy.

Skimming Operation

High Tech investigators assisting a local police agency who arrested a suspect of Romanian decent involved in a skimming operation, were successfully able to conduct a forensics examination of his cellular telephone and GPS device. The evidence, several hundred text messages in Romanian, will be a crucial point of the investigation as well as the route information extracted from the GPS device. The route information identified several shopping centers the suspect frequented to install the skimming devices which were found in his car at the time of his arrest. As a result of the forensics examinations, the investigating police agency was able to locate and remove an installed skimming device from an ATM.

Unlawful Access

High Tech investigators became involved in an investigation that focused on suspects who intruded and unlawfully accessed the personal email account of a former well-known model and a major league baseball player. Personal photographs were posted on the Internet in an effort to cause the victims harm. Investigators served multiple search warrants that confirmed the victim's email account had been unlawfully accessed. The point of compromise was traced to a city in Minnesota. Authorities in

Minnesota executed a search warrant at a private residence identified by the Task Force. The suspect was identified by Minnesota authorities as a 19-year-old college student. A forensic examination of her laptop computer revealed the compromised photographs. Charges were filed against the student by Minnesota authorities.

Fraud

A suspect falsely represented himself as a representative of Dolby Laboratories with the intent to defraud the company of computer components. The suspect used a scheme he had concocted to solicit business partners for a newly-created Dolby Home Theater division of Dolby. This new company was set to be unveiled at an annual computer show in Las Vegas, Nevada. He marketed offers of free licensing, free software, and waived royalty fees as lures he used to bait companies into donating high-end computer components he claimed were needed to build high-end systems to use at the official unveiling. The suspect provided a fictitious Dolby licensing contract to one of the companies. In the course of the investigation, the suspect was inadvertently tipped off by Dolby's initial investigation. The suspect, a convicted felon who had served time in a California state prison, contacted Dolby and partially confessed his illegal activity in an effort to control the damage. Investigators identified multiple companies who provided the suspect with items such as computer components and peripherals needed to construct high-grade computer systems.

Skimming

High Tech investigators responded to Universal City regarding a skimming case involving NBC Studios. Universal Studios security and NBC Studios security realized that their studios systems suffered intrusions targeting personal employee information. Losses are reported in excess of $100,000. Three suspects were identified.

Forensic Examination

A forensics examination of a suspected identity thief's computer led to the discovery of an armed robbery. The investigator found the suspect's photograph on a bank robbery wanted bulletin electronically saved in the suspect's files under "my photos." A simple Internet search with date, time, and file information listed on the bulletin revealed that it was published by the FBI. It was determined the suspect "copied" and "pasted" the bulletin into his computer files. Through this information, the location of the bank was identified. The robbery information, and evidence results to the identity theft crimes originally investigated, was released to the Identity Theft Task Force detective. The investigator ultimately alerted the FBI regarding the robbery information. FBI investigators are pursing their investigation and case filing. The Los Angeles County District Attorney's office filed identity theft charges against the suspect.

Credit and Debit Card Skimming

A business owner and his wife, operating in Los Angeles County, conspired with others to skim credit and debit cards from several locations. The skimmed information was used to make hundreds of purchases, including the purchase of items to run their own business. The investigation led to the service of multiple search warrants which exposed this investigation as part of a larger group of thieves installing skimming

devices at gas station pumps and using the information they obtained to manufacture counterfeit credit cards. Illegal weapons, skimming devices, profiles, and $40,000 in cash were seized.

Identity Theft

Identity Theft investigators arrested a merchant responsible for processing in excess of $30,000 in fraudulent charges using his business' merchant account. The compromised accounts involved Federal Express as well as cards bearing the MasterCard and Visa logos. The merchant was arrested following the investigation which revealed that he received a percentage of the fraudulent charges authorized. The percentage was paid by other suspects who unlawfully obtained personal identifying information and used it to counterfeit credit cards, which were processed by the merchant. Losses exceeded $100,000.

Credit Card Fraud

Las Vegas authorities issued high-dollar arrest warrants for two suspects that passed over $200,000 in non-sufficient fund checks at several casinos on the Las Vegas Strip. The Task Force obtained information from a reliable informant that the suspects were staying at a residence in the San Gabriel area. Surveillance was conducted which confirmed the suspects whereabouts. A search/arrest warrant was executed and both suspects were located. The suspects were in possession of fraudulently obtained credit cards, identifications, and one-way tickets to China with a departure time for later that afternoon. Needless to say, their trip was postponed and they were extradited back to Nevada where they stood trial.

Identity Theft

Investigators worked alongside Home Depot investigators after a victim reported that someone used her personal identifying information to obtain a fraudulent credit card, and purchased a refrigerator. Home Depot assisted investigators in the coordination of a controlled delivery. Investigators delivered the refrigerator and arrested the suspects following the service of a search warrant. The suspects possessed the victim's personal information along with credit cards in her name, which included the card used to purchase the refrigerator.

Identity Theft

The Secret Service assisted in the seizure of luxury vehicles possessed by a suspect who had been the subject of an identity theft investigation involving the manufacturing of credit cards. The luxury vehicles, worth in excess of $160,000 (combined), were part of an asset forfeiture claim. Since the suspect was on felony probation, a probation search was also conducted. A large amount of money was confiscated as well as additional credit cards and software to manufacture credit cards. The suspect and his attorney have made arrangements to cooperate with the investigator and they have expressed their intent to identify the supplier.

Credit Card Fraud
Patrol deputies arrested a person who was also in possession of credit card numbers. Investigators identified 25,000 credit card numbers; 14,000 of which belonged to Bank of America. Each of the numbers were authenticated and legitimately issued by the bank. Investigators determined that the suspect obtained the numbers fraudulently using a software program called Credit Wizard, a European based credit card generator.

Credit Card Theft
Investigators served a search warrant targeting a suspect involved in the theft of new credit cards from a legitimate manufacturer contracted by banking institutions. The suspects, working together, developed a plan to identify shipments of cards for delivery to the various banks. The cards were stolen in bulk quantities with activation information. The case involves an insider.

Identity Theft
A suspect obtained personal identifying information and used it to fraudulently purchase two homes. The suspect rented the homes with the intent of reselling (flipping) the properties. Unfortunately, the real estate market was impacted by the economy forcing the renters to vacate. When that happened, the suspect defaulted on the mortgage payments. The incident was discovered when the victim applied for credit and her credit history revealed the properties in her name.

Identity Theft
Investigators arrested two identity thieves and served a search warrant after it was learned the suspects used stolen identities to create fictitious businesses and obtain merchant credit charge accounts. The suspects then obtained stolen international credit card numbers and processed them through the merchant accounts they established. One of the suspects, and a source of the stolen profiles, worked at an insurance company. She confessed. The investigation revealed that additional suspects established bank accounts withdrawing against the stolen funds. The investigation identified 30 identity theft victims whose profile information was used to open 75 fraudulent accounts. Investigators determined that 300 stolen credit card numbers were obtained contributing in over $200,000 in credit card losses.

Identity Theft
Investigators arrested two suspects for using the personal identifying information of a U.S. Army Iraq War veteran. One of the suspects used the information to gain employment while the other used the information to avoid criminal prosecution. Subsequently, through the actions of both suspect, the victim incurred an arrest record and numerous warrants for his arrest. Efforts have been made to find the victim “factually innocent” of the events.

Jail Phone Fraud
Investigators identified inmates associated with the 36th Street gang who used jail phones to place fraudulent calls using a given number supplied to them. An outside

operator would forward the calls worldwide. Losses were documented in excess of $70,000. The Los Angeles County District Attorney's Office filed 18 felony counts of fraud against the suspects in the case labeled, *Jail Operator*.

Stolen Credit Card Profiles

Investigators working on information from the Federal Bureau of Investigation (FBI) acted on information that identity thieves were fraudulently ordering event tickets using stolen credit card profiles. A $10,000 transaction was identified and a sting operation was coordinated with the assistance of American Express. One suspect was arrested when he appeared at a pre-designated place to pick up an event order. The suspect shared with investigators during his interview that he was involved with a theft ring that purchases $10,000 to $50,000 in event tickets. The purchases occurred on a regular basis throughout the United States using credit card information obtained from skimmed credit card locations. The suspect(s) then scalp the tickets on the day of the event for two to five times their actual value.

Identity Theft

Identity Theft investigators obtained a federal indictment on a suspect for aggravated identity theft (Title 18 USC 1028A). Through the use of informants, and a trap and trace on his phone, the suspect was located in Las Vegas, Nevada. The suspect was arrested by the Nevada FBI field office and extradited to California. The suspect is part of a West African criminal group operating in the Southern California and Las Vegas area. The group is responsible for large sophisticated mail theft schemes using postal employees, data intrusion, and real estate fraud.

Identity Theft investigators arrested a suspect at a Los Angeles area Home Depot store following a surveillance and sting operation. The suspect compromised identities of persons living in southern California and he was making fraudulent purchases throughout Los Angeles. Stolen property and firearms were recovered during a search warrant of his residence. In a surprise discovery, investigators found hidden access to a room in a garage. The room was used to grow marijuana using hydroponics technology (method of using timed irrigation and heat lamps to simulate outdoor growing environments). The equipment and 65 marijuana plants were confiscated as evidence. The suspect's 10-year-old daughter was home alone during this incident.

Credit Card Skimming Plant

Identity Theft investigators dismantled a credit card skimming plant in the city of Los Angeles. Investigators acted on information and conducted a surveillance of a location allegedly involved in a skimming operation. Several traffic stops were made of vehicles that left the location. Four suspects, in possession of credit cards, were arrested during these stops. A search warrant was served at the location, a warehouse, and investigators discovered the skimming operation. Personal profiles, credit cards and card stock, and equipment to encode the cards were confiscated as evidence. Seven arrests were made.

Telecommunications Fraud

A suspect was convicted and sentenced to five years in prison. He was involved in a large telecommunications fraud/identity theft case in which SBC/AT&T was defrauded out of $2,000,000. The suspect created his own “mini phone company” and used stolen identities to set up high-capacity phone lines which were used to forward toll calls to Cuba, Somalia, and Syria.

Identity Theft

Investigators executed a search warrant at the residence of a suspect who used the California Secretary of State website to search for corporations whose licenses were suspended. Once he identified a suspended corporate licensee, he would associate the license to the person it was registered to. Ultimately, the registrant became a victim of identity theft. The suspect would renew the businesses charter and then resell the corporation’s identity. The renewed corporation’s identity had value because of their established credit history which would aid the new owner in facilitating credit approval. The dollar losses are in excess of a million dollars.

Mortgage Fraud/Computer Intrusion

A suspect in a mortgage fraud/computer intrusion case pled guilty to felony charges of computer intrusion and identity theft. The case involved a Securities and Investments Department employee for Wachovia Bank, who accessed the computer system, and printed out account information for approximately thirty high-dollar account holders. Documents were sold to third parties in attempt to facilitate identity fraud. The former employee was sentenced to three years in prison.

Identity Theft

Investigators with the assistance of the FBI, Glendale PD, LAPD, served a three location search warrant and conducted a takedown of four prolific identity theft suspects in operation “Big Skim.” The case is part of a four-year investigation that has already resulted in numerous arrests, seizures and the forfeiture of cash and millions of dollars in stolen merchandise. A Ferrari, a Porsche, a BMW, an Escalade, and $40,000 in cash were among items seized. In addition, several high-tech Bluetooth skimmers, hundreds of counterfeit credit cards and profiles, computers, electronics and cellular phones were confiscated as evidence. To date, over 15,000 accounts have been confirmed

compromised along with the locations of 14 gas stations where the crimes were committed. The loss has been estimated at $3,000,000.

False Impersonation
Investigators assisted a victim of a false impersonation. The victim, a military veteran, had been troubled by this event for 13 years. The suspect amassed several warrants under the victim's name. The victim was arrested twice for actions taken by the suspect. The suspect was arrested and sentenced to 16 months in state prison.

Gift Card Theft
Investigators conducted two search warrants in the city of Los Angeles in response to an investigation involving the theft of American Express gift cards from a UPS hub. The thefts were a regular occurrence as thieves knew that the company manufacturing the cards used UPS as the shipper. The UPS employee was identified following the interviews that took place after the service of the warrants. The UPS employee's residence was searched and American Express gift cards were recovered.

Operation Big Skim
The International Association of Financial Crimes Investigators recognized the Task Force for the successful skimming investigation dubbed "Operation Big Skim". The investigation involved the arrest and prosecution of 12 suspects who defrauded financial institutions and major oil companies out of $4.5 million. The investigation involved surveillance operations and undercover operations ultimately netting the seizure of approximately $342,000 and high-end vehicles (BMW's, Porches, Ferrari's and a Rolls Royce) valued at $450,000. Some members of this elaborate group were loosely connected to the Arellano Felix Cartel and they operated nationwide. In addition to the skimming operation, the suspects were also involved in cargo thefts, which led investigators to the recovery of over $1 million in stolen high tech cargo. One of these cargo thefts was extremely violent. The driver of the big rig was kidnapped at gunpoint. The driver's hands were bound with duct tape and he was thrown out of his truck in Southern Los Angeles County. Numerous location search warrants were served and five large credit card manufacturing plants were dismantled which were operated by this group. The Task Force identified over 50,000 victims and over 65 merchant Credit Card Processor services.

Identity Theft
Identity Theft investigators served two search warrants in the cities of Long Beach and Harbor City. The suspects used the stolen corporate identity of US Welding Works to open a virtual office suite in Colorado and apply for a line of credit with Home Depot. The case is being investigated in conjunction with the US Secret Service and the Colorado Bureau of Investigations. The estimated loss so far exceeds $74,000. Two suspects were arrested

Identity Theft
Identity Theft investigators, working with FBI investigators, served a search warrant in the city of North Hollywood. A suspect involved in credit card skimming and decoding

was arrested. Profiles, card stock, and fraudulent identifications were seized at the location.

Identity Theft
Identity Theft investigators served a search warrant at the home of a bank teller. The teller had unofficially accessed customer bank accounts without their consent or knowledge. The accounts were used to divert stolen funds from fraudulent credit card transactions. The teller was also questioned regarding a recent robbery at the bank. The teller on duty gave money to the robber and failed to include the dye pack or activate the alarm. The teller provided useful information to investigators.

Identity Theft
Identity Theft investigators assisted the US Secret Service with a large scale identity theft case involving insiders from various banks. It was also discovered the case involves suspects from a previous investigation dubbed “Bad Boy,” reported in 2005. Numerous suspects were identified throughout Southern California.

Identity Theft
Identity Theft investigators were notified by American Express that a stolen card was used at a local hotel. The stolen credit card was linked to a case involving 32 additional victims. Investigators responded to the hotel and arrested two suspects in possession of 50 additional counterfeit cards, an encoding machine, and a laptop computer. The suspects were also in possession of methamphetamine.

Computer and Technology Crime High-Tech Response Team (CATCH)

Lead Agency: **San Diego County District Attorney's Office**
CATCH is represented by the following three counties with a combined population of more than 5 million:

- Imperial
- Riverside
- San Diego

Through a common memorandum of understanding, CATCH is comprised of participants from the following agencies:

- California Department of Justice
- California Department of Motor Vehicles
- Carlsbad Police Department
- Chula Vista Police Department
- Federal Bureau of Investigation
- Imperial County District Attorney's Office
- Riverside County District Attorney's Office
- Riverside County Sheriff's Department
- San Diego County District Attorney's Office
- San Diego County Probation Department
- San Diego County Sheriff's Department
- San Diego Police Department
- U.S. Postal Inspection Service
- U.S. Secret Service

CATCH Case Profiles:

San Diego Superior Court Case #SCD227265
The suspect in this case advertised that he could modify game consoles and had thousands of software titles for sale. An undercover buy yielded a modified console and 58 pirated games. A second undercover operation and follow up warrant resulted in the seizure of a number of drives and computer equipment. The forensic examination of the suspect's computers revealed 14,000 pirated game titles from Sony and ESA at an estimated loss of $86,000.

On November 7, 2010, CATCH was recognized with an award in the law enforcement category for being one of the most outstanding organizations in San Diego working to enhance cyber security on behalf of the public at the Securing our eCity, cyber security symposium. The Securing our eCity initiative was recently recognized as one of the winners of the National Cybersecurity Awareness Challenge's best local/community plans.

San Diego Superior Court Case #SCD223097
The suspect used victims' phone numbers to file hundreds of fraudulent claims for lost or damaged cell phones, paid the deductable, and obtained "replacement" phones, which he sold. The suspect shipped over a thousand phones to 12 different addresses from June of 2007 until September of 2009, with an estimated $388,669 in losses.

On March 20, 2010, the *San Diego Union-Tribune* listed CATCH as one of the key places in the region to turn for help when victimized. The article was entitled, "What if I've been scammed?" and described several of the recent fraud scams.

San Diego Superior Court Case #SCD226349
The suspect used peer-to-peer networks to obtain and trade personal identifying information of others, including tax forms and financial documents. The suspect exploited a setting that shares the entire drive and bypassing security features, of the victims' networks, downloaded their financial documents. The victims number in the hundreds and are located across the United States. The suspect was on probation for a prior identity theft case.

San Diego Superior Court Case #SCD223311
The suspect advertised Apple computers for sale pre-loaded with software. During an undercover buy, investigators purchased a computer loaded with pirated software. The computer was originally purchased with a stolen credit card. A second computer was purchased from the suspect on a controlled buy and it was also loaded with pirated software. A subsequent search located 30 brand new Apple computers still in their original boxes and pirated software from Microsoft, Apple and Adobe.

California Department of Justice
Advanced Training Center

During the 2009/2010 training year, the California Department of Justice, Advanced Training Center (ATC) continued to be a leader in conducting specialized training courses to the law enforcement community assigned to investigate high technology crimes. It is no secret that terrorist and criminal organizations take advantage of society's dependence on technology to further their goals of disruption and theft on a massive scale, and the ATC takes pride in its role of providing cutting-edge training to hundreds of law enforcement professionals to combat this threat.

The ATC presented seven relevant computer crime and cyber terrorism training courses to law enforcement agencies throughout California. These specialized courses brought to the law enforcement community the latest technology coupled with the real world experience of ATC's highly skilled instructors. These instructors are subject matter experts in the field and are assigned cases due to their knowledge of investigating high technology crimes.

The methods and technologies used by persons committing computer crimes and cyber terrorism are constantly evolving. In order to provide law enforcement agencies the most current information on these trends and technologies, the ATC constantly researches and updates the courses to include up-to-date information. Because the investigations of these particular crimes are complex, the ATC instructors spared no effort during the training sessions to ensure the students fully comprehended the course material prior to proceeding to the next topic. By utilizing adult learning theories during the presentation of the courses, the students experienced "real life scenarios" while in a controlled classroom setting. This allowed the students to have a complete understanding of the course material so they can successfully apply these technologies and techniques in real law enforcement investigations.

The relevance of continued training in areas of electronic evidence also plays a major role in everyday investigations. Most crimes today have some related electronic evidence whether it is a computer, cell phone, instant chat, email, flash drive, digital camera, or digital pictures. Investigators continually need up-to-date tools and training in order to adapt to the changing criminal environment to fully understand how electronic evidence plays a vital role in everyday investigations. The ATC is well aware of the importance technology plays and strives to continue to be on the forefront of training in order to give law enforcement the edge it needs to stay on top of electronic evidence and to improve the process and use of evidence found in order to provide the best possible investigative service.

The ATC understands the reality of the current fiscal crisis and its effects on law enforcement agency training budgets. To assist agencies in reducing their travel costs, the ATC presented courses in both southern and northern California. Members of the five California High Technology Task Force agencies (Computer & Technology Crimes

High-Tech Response Team – San Diego; Northern California Computer Crimes Task Force – Napa; Rapid Enforcement Allied Computers Team – Santa Clara; Sacramento Valley Hi-Tech Crimes Task Force - Sacramento; and Southern California Rapid Enforcement Allied Computer Team – Norwalk), were given first priority to this training, and the remaining seats were offered to agencies not associated to a task force.

The following is a list of courses the ATC presented:

PC Forensics - Data Collection

This course introduced the students to the unique skills, best practices and methodologies necessary to assist in the investigation and prosecution of computer crimes. The course consists of lectures, presentations and hands-on classroom exercises on such topics as Partitioning, Formatting, Data Storage, Hardware and Software Write Blockers, the "Boot Up" Process and Duplicate Imaging.

Santa Barbara – September 2009
Rancho Cordova – April 2010

PC Forensics - Specialized Investigative Tools

This course provided investigators with the necessary training, skills, knowledge and practical experience in using some of the more advanced tools developed for computer forensics. The training also included how to make image files of digital evidence and how to verify that changes were not made to the evidence while conducting the investigation.

Pasadena October – 2009

Computer Crimes/LAN Investigation

This course was designed to teach law enforcement investigators the principals of responding to and investigating network intrusion crimes. Students created a Local Area Network (LAN) and a Wide Area Network (WAN) to study. Concepts of the Global Area Network (GAN) were discussed to help understand how exploits and hacks of networked systems are committed.

Camarillo – January 2010

PC Forensics - Investigations Advanced for the Investigator

This course was designed to provide investigators of high technology and/or computer crimes training on tools and procedures for conducting difficult and detailed forensic examinations of personal computers and seized digital media. Students also learned how to build their own forensic analysis computer, troubleshoot and repair problems with their computers, and become familiar with advanced capabilities of tools available to the forensic analyst. The course consisted of lecture, hands-on classroom exercises, and 70 to 75 hours of lab work.

Rancho Cordova – December 2009
Orange – May 2010

Cellular Phone Forensics/Investigations

The course provided law enforcement personnel with foundational skills and knowledge necessary for the forensic examination of cellular phones. When special circumstances arise, special consideration has to be given when a cellular phone is used as an instrument of crime or when a cellular phone contains records of criminal activity. These records can be in many forms including, but not limited to; phonebook entries, call history, text messages, calendar entries, images and videos. This course was designed to help the investigator by giving the students a foundation for cellular phone forensics to better understand and respond to these types of criminal activity.

Rancho Cordova – January 2010

Computer Forensics-Macintosh/Linux – Development Session

The session was used for the development of other ATC courses within the high technology class series. This enabled the ATC to keep class materials updated and ready for presentation. In addition, one of the ATC's classroom labs was updated in order to stay current with ever-changing technology, specifically forensic software compatibility.

Huntington Beach – June 2010

Course evaluations received from the aforementioned courses have shown the material and training that were presented was beneficial to both seasoned and new officers assigned to high technology units. These training courses could not be possible without the partnerships between the ATC and the leading forensic software companies such as Guidance Software Inc, AccessData, and Susteen, Inc. Partnerships with these companies have been beneficial in keeping training affordable by the reduced costs in the software packages utilized in the courses. This forensic software is provided to the graduating students to take back to their respective agencies to help them investigate high technology cases affecting California's citizens.

California Department of Justice
Deputy Attorney General
HTTAP Support

There are five Deputy Attorney Generals (DAGs) and one Special Agent assigned to support the High Technology Theft, Apprehension, and Prosecution Program. One DAG is assigned to support each of the five task forces. The duties of the DAGs include:

1) Prosecution support to the five task forces;
2) Development and delivery of training programs to law enforcement and the public;
3) Legal and prosecution support to rural counties;
4) Coordination of out-of-state investigation requests; and
5) State agency legal and prosecution support.

During fiscal year 2009/2010, the DAGs:

- Initiated nine investigations
- Filed one indictment
- Filed 16 complaints
- Aggregate loss to the victims exceeded $2,800,000
- Convicted 29 defendants
- Sentenced 30 defendants
- Court ordered restitution was in the amount of $1,108,225
- Provided 19 training sessions on cyber crime issues

The expansion of the program's targeted offenses from identity theft to cybercrime has assisted the Attorney General's Office in being more responsive to the State's High Technology Theft, Apprehension, and Prosecution Program as well as local and state government agencies. The program has provided assistance on a number of diverse issues including Google's Wi-Fi Street View interception issues and the legality of use of a passive audio/video phone that is deployed by hostage negotiators.

The project is also assisting with the Prosecutors' Encyclopedia (PE). PE is a closed Wikipedia for law enforcement and prosecutors. PE is a project of the New York Prosecutors Training Institute in partnership with state, federal, and a number of prosecutor organizations. PE is intended not only to provide resources but to facilitate collaboration among prosecutors from across the United States.

California District Attorneys Association

The California District Attorneys Association (CDAA) employs HTTAP funds to continue developing and presenting its high tech crime prosecution training program. CDAA's efforts augment and enhance statewide efforts to combat online fraud, identity theft and other crimes perpetrated with the use of high technology by providing task force personnel and others with the specialized training needed to effectively address the evolving and complex problems often posed by these offenses.

CDAA's program provides training to prosecutors and law enforcement officers from all California counties. The training is multi-disciplinary and targets the successful investigation, apprehension, and prosecution of criminal organizations, networks, and individuals involved in high technology and computer-based crimes. CDAA complements this program with an ongoing series of publications and legal updates.

CDAA's HTTAP funds support the following specific activities:

- Development and publication of CDAA's high technology crimes newsletter, ***Firewall,*** which highlights emerging issues, relevant legislative updates, pertinent court cases and upcoming training opportunities.
- Production and distribution of California's first high tech crime prosecution practice guide, ***Investigation and Prosecutions of High Tech Crimes.*** The manual is currently distributed on CD-ROM.
- Development and maintenance of online resources including:
  - A PowerPoint and audio library available to all California prosecutors;
  - A brief bank which currently houses over 300 high-technology briefs, points and authorities, and court cases;
  - An expert witness database containing 850 documents including transcripts, articles, briefs, and curricula vita on over 100 different experts; and
  - A project website which provides all California prosecutors with updated resources guides and links to the various other sources mentioned above.
- Providing *ad hoc* technical and legal assistance to California prosecutors and investigators who must respond to unforeseen high tech crime problems in court and in the field.
- Providing training to over 75 prosecutors throughout the state of California at three different training courses. Two of those trainings included "hands-on" interaction (thanks to the cooperative use of a mobile computer lab provided by California Department of Justice's Advanced Training Center).
- CDAA has also initiated webinar training sessions for prosecutors who cannot attend in person. These high-quality and informative trainings are provided in "real time" and delivered to participating students' individual desktops.

A total of $260,420 was awarded to CDAA in furtherance of these activities. This amount includes a 25 percent match of $52,096.

California Penal Code Sections 13848-13848.8.

13848. (a) It is the intent of the Legislature in enacting this chapter to provide local law enforcement and district attorneys with the tools necessary to successfully interdict the promulgation of high technology crime. According to the federal Law Enforcement Training Center, it is expected that states will see a tremendous growth in high technology crimes over the next few years as computers become more available and computer users more skilled in utilizing technology to commit these faceless crimes. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or which is the target of a criminal act.

(b) Funds provided under this program are intended to ensure that law enforcement is equipped with the necessary personnel and equipment to successfully combat high technology crime which includes, but is not limited to, the following offenses:

(1) White-collar crime, such as check, automated teller machine, and credit card fraud, committed by means of electronic or computer-related media.

(2) Unlawful access, destruction of or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wireline communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, or unauthorized disclosure of data stored within those computers and networks.

(3) Money laundering accomplished with the aid of computer networks or electronic banking transfers.

(4) Theft and resale of telephone calling codes, theft of telecommunications service, theft of wireless communication service, and theft of cable television services by manipulation of the equipment used to receive those services.

(5) Software piracy and other unlawful duplication of information.

(6) Theft and resale of computer components and other high technology products produced by the high technology industry.

(7) Remarking and counterfeiting of computer hardware and software.

(8) Theft of trade secrets.

(c) This program is also intended to provide support to law enforcement agencies by providing technical assistance to those agencies with respect to the seizure

and analysis of computer systems used to commit high technology crimes or store evidence relating to those crimes.

13848.2. (a) There is hereby established in the agency or agencies designated by the Director of Finance pursuant to Section 13820 a program of financial and technical assistance for law enforcement and district attorneys' offices, designated the High Technology Theft Apprehension and Prosecution Program. All funds appropriated to the agency or agencies designated by the Director of Finance pursuant to Section 13820 for the purposes of this chapter shall be administered and disbursed by the executive director of the office in consultation with the High Technology Crime Advisory Committee as established in Section 13848.6 and shall to the extent feasible be coordinated with federal funds and private grants or private donations that are made available for these purposes.

(b) The Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 is authorized to allocate and award funds to regional high technology crime programs which are established in compliance with Section 13848.4.

(c) The allocation and award of funds under this chapter shall be made on application executed by the district attorney, county sheriff, or chief of police and approved by the board of supervisors for each county that is a participant of a high technology theft apprehension and prosecution unit.

(d) In identifying program areas that will be eligible for competitive application during the 1998-99 fiscal year for federal funding pursuant to the Edward Byrne Memorial State and Local Law Enforcement Assistance Programs (Subchapter V (commencing with Section 3750) of Chapter 46 of the United States Code), the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall include, to the extent possible, an emphasis on high technology crime by selecting funding areas that would further the use of federal funds to address high technology crime and facilitate the establishment of high technology multijurisdictional task forces.

(e) The agency or agencies designated by the Director of Finance pursuant to Section 13820 shall allocate any increase in federal funding pursuant to the Anti-Drug Abuse Act (Public Law 100-690) for the 1998-99 fiscal year to those programs described in subdivision (d).

13848.4. (a) All funds appropriated to the agency or agencies designated by the Director of Finance pursuant to Section 13820 for the purposes of this chapter shall be deposited in the High Technology Theft Apprehension and Prosecution Program Trust Fund, which is hereby established. The fund shall be under the direction and control of the executive director. Moneys in the fund, upon appropriation by the Legislature, shall be expended to implement this chapter.

(b) Moneys in the High Technology Theft Apprehension and Prosecution Program Trust Fund shall be expended to fund programs to enhance the capacity of

local law enforcement and prosecutors to deter, investigate, and prosecute high technology related crimes. After deduction of the actual and necessary administrative costs referred to in subdivision (f), the High Technology Theft Apprehension and Prosecution Program Trust Fund shall be expended to fund programs to enhance the capacity of local law enforcement, state police, and local prosecutors to deter, investigate, and prosecute high technology related crimes. Any funds distributed under this chapter shall be expended for the exclusive purpose of deterring, investigating, and prosecuting high technology related crimes.

(c) Up to 10 percent of the funds shall be used for developing and maintaining a statewide database on high technology crime for use in developing and distributing intelligence information to participating law enforcement agencies. In addition, the Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 may allocate and award up to 5 percent of the funds available to public agencies or private nonprofit organizations for the purposes of establishing statewide programs of education, training, and research for public prosecutors, investigators, and law enforcement officers relating to deterring, investigating, and prosecuting high technology related crimes. Any funds not expended in a fiscal year for these purposes shall be distributed to regional high technology theft task forces pursuant to subdivision (b).

(d) Any regional task force receiving funds under this section may elect to have the Department of Justice administer the regional task force program. The department may be reimbursed for any expenditures incurred for administering a regional task force from funds given to local law enforcement pursuant to subdivision (b).

(e) The agency or agencies designated by the Director of Finance pursuant to Section 13820 shall distribute funds in the High Technology Theft Apprehension and Prosecution Program Trust Fund to eligible agencies pursuant to subdivision (b) in consultation with the High Technology Crime Advisory Committee established pursuant to Section 13848.6.

(f) Administration of the overall program and the evaluation and monitoring of all grants made pursuant to this chapter shall be performed by the agency or agencies designated by the Director of Finance pursuant to Section 13820, provided that funds expended for these functions shall not exceed 5 percent of the total amount made available under this chapter.

13848.6. (a) The High Technology Crime Advisory Committee is hereby established for the purpose of formulating a comprehensive written strategy for addressing high technology crime throughout the state, with the exception of crimes that occur on state property or are committed against state employees, and to advise the agency or agencies designated by the Director of Finance pursuant to Section 13820 on the appropriate disbursement of funds to regional task forces.

(b) This strategy shall be designed to be implemented through regional task forces. In formulating that strategy, the committee shall identify various priorities for law enforcement attention, including the following goals:

(1) To apprehend and prosecute criminal organizations, networks, and groups of individuals engaged in the following activities:

(A) Theft of computer components and other high technology products.

(B) Violations of Penal Code Sections 211, 350, 351a, 459, 496, 537e, 593d, and 593e.

(C) Theft of telecommunications services and other violations of Penal Code Sections 502.7 and 502.8.

(D) Counterfeiting of negotiable instruments and other valuable items through the use of computer technology.

(E) Creation and distribution of counterfeit software and other digital information, including the use of counterfeit trademarks to misrepresent the origin of that software or digital information.

(2) To apprehend and prosecute individuals and groups engaged in the unlawful access, destruction, or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wire line communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, and unauthorized disclosure of data stored within those computers.

(3) To apprehend and prosecute individuals and groups engaged in the theft of trade secrets.

(4) To investigate and prosecute high technology crime cases requiring coordination and cooperation between regional task forces and local, state, federal, and international law enforcement agencies.

(c) The Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall appoint the following members to the committee:

(1) A designee of the California District Attorneys Association.

(2) A designee of the California State Sheriffs Association.

(3) A designee of the California Police Chiefs Association.

(4) A designee of the Attorney General.

(5) A designee of the California Highway Patrol.

(6) A designee of the High Technology Crime Investigation Association.

(7) A designee of the agency or agencies designated by the Director of Finance pursuant to Section 13820.

(8) A designee of the American Electronic Association to represent California computer system manufacturers.

(9) A designee of the American Electronic Association to represent California computer software producers.

(10) A designee of the California Cellular Carriers Association.

(11) A representative of the California Internet industry.

(12) A designee of the Semiconductor Equipment and Materials International.

(13) A designee of the California Cable Television Association.

(14) A designee of the Motion Picture Association of America.

(15) A designee of either the California Telephone Association or the California Association of Competitive Telecommunication Companies. This position shall rotate every other year between designees of the two associations.

(16) A representative of the California banking industry.

(17) A representative of the Office of Privacy Protection.

(18) A representative of the Department of Finance.

(d) The Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall designate the Chair of the High Technology Crime Advisory Committee from the appointed members.

(e) The advisory committee shall not be required to meet more than 12 times per year. The advisory committee may create subcommittees of its own membership,

and each subcommittee shall meet as often as the subcommittee members find necessary. It is the intent of the Legislature that all advisory committee members shall actively participate in all advisory committee deliberations required by this chapter.

Any member who, without advance notice to the executive director and without designating an alternative representative, misses three scheduled meetings in any calendar year for any reason other than severe temporary illness or injury (as determined by the Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820) shall automatically be removed from the advisory committee. If a member wishes to send an alternative representative in his or her place, advance written notification of this substitution shall be presented to the executive director. This notification shall be required for each meeting the appointed member elects not to attend.

Members of the advisory committee shall receive no compensation for their services, but shall be reimbursed for travel and per diem expenses incurred as a result of attending meetings sponsored by the agency or agencies designated by the Director of Finance pursuant to Section 13820 under this chapter.

(f) The executive director, in consultation with the High Technology Crime Advisory Committee, shall develop specific guidelines and administrative procedures for the selection of projects to be funded by the High Technology Theft Apprehension and Prosecution Program, which guidelines shall include the following selection criteria:

(1) Each regional task force that seeks funds shall submit a written application to the committee setting forth in detail the proposed use of the funds.

(2) In order to qualify for the receipt of funds, each proposed regional task force submitting an application shall provide written evidence that the agency meets either of the following conditions:

(A) The regional task force devoted to the investigation and prosecution of high technology-related crimes is comprised of local law enforcement and prosecutors, and has been in existence for at least one year prior to the application date.

(B) At least one member of the task force has at least three years of experience in investigating or prosecuting cases of suspected high technology crime.

(3) Each regional task force shall be identified by a name that is appropriate to the area that it serves. In order to qualify for funds, a regional task force shall be comprised of local law enforcement and prosecutors from at least two counties. At the time of funding, the proposed task force shall also have at least one investigator assigned

to it from a state law enforcement agency. Each task force shall be directed by a local steering committee composed of representatives of participating agencies and members of the local high technology industry.

(4) The California High Technology Crimes Task Force shall be comprised of each regional task force developed pursuant to this subdivision.

(5) Additional criteria that shall be considered by the advisory committee in awarding grant funds shall include, but not be limited to, the following:

(A) The number of high technology crime cases filed in the prior year.

(B) The number of high technology crime cases investigated in the prior year.

(C) The number of victims involved in the cases filed.

(D) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, or corporations, as a result of the high technology crime cases filed, and those under active investigation by that task force.

(6) Each regional task force that has been awarded funds authorized under the High Technology Theft Apprehension and Prosecution Program during the previous grant-funding cycle, upon reapplication for funds to the committee in each successive year, shall be required to submit a detailed accounting of funds received and expended in the prior year in addition to any information required by this section. The accounting shall include all of the following information:

(A) The amount of funds received and expended.

(B) The use to which those funds were put, including payment of salaries and expenses, purchase of equipment and supplies, and other expenditures by type.

(C) The number of filed complaints, investigations, arrests, and convictions that resulted from the expenditure of the funds.

(g) The committee shall annually review the effectiveness of the California High Technology Crimes Task Force in deterring, investigating, and prosecuting high

technology crimes and provide its findings in a report to the Legislature and the Governor. This report shall be based on information provided by the regional task forces in an annual report to the committee which shall detail the following:

(1) Facts based upon, but not limited to, the following:

(A) The number of high technology crime cases filed in the prior year.

(B) The number of high technology crime cases investigated in the prior year.

(C) The number of victims involved in the cases filed.

(D) The number of convictions obtained in the prior year.

(E) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, corporations, and other relevant public entities, according to the number of cases filed, investigations, prosecutions, and convictions obtained.

(2) An accounting of funds received and expended in the prior year, which shall include all of the following:

(A) The amount of funds received and expended.

(B) The uses to which those funds were put, including payment of salaries and expenses, purchase of supplies, and other expenditures of funds.

(C) Any other relevant information requested.

13848.8. (a) The executive director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall also appoint the following members to the High Technology Crime Advisory Committee established by Section 13848.6:

(1) A designee of the Recording Association of America.

(2) A designee of the Consumers Union.

(b) The High Technology Crime Advisory Committee, in formulating a comprehensive written strategy for addressing high technology crime throughout the state, shall identify, in addition to the various priorities for law enforcement attention specified in subdivision (b) of Section 13848.6, the goal of apprehending and

prosecuting criminal organizations, networks, and groups of individuals engaged in the following activities:

(1) Violations of Sections 653h, 653s, and 635w.

(2) The creation and distribution of pirated sound recordings or audiovisual works or the failure to disclose the origin of a recording or audiovisual work.

HTCAC BYLAWS
STATE OF CALIFORNIA
BYLAWS, RULES AND PROCEDURES
OF THE HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE
Adopted: June 2005
Revised: December 2008

ARTICLE I: NAME AND AUTHORITY

This organization, created in the State government by statutory authority, shall be known as the High Technology Crime Advisory committee – hereinafter referred to as the "Committee."

ARTICLE II: MEMBERSHIP AND CHAIRPERSON SELECTION

Section 1.
The Committee shall include the following twenty one representatives:
(1) A designee of the California District Attorneys Association;
(2) A designee of the California State Sheriff's Association;
(3) A designee of the California Police Chief's Association;
(4) A designee of the California Attorney General;
(5) A designee of the California Highway Patrol;
(6) A designee of the High Technology Crime Investigation Association;
(7) A designee of the California Office of Emergency Services;
(8) A designee of the American Electronic Association to represent California computer system manufacturers;
(9) A designee of the American Electronic Association to represent California software producers;
(10) A designee of the CTIA – The Wireless Association;
(11) A designee of the California Internet Industry;
(12) A designee of the Semiconductor Equipment and Materials International (SEMI);
(13) A designee of the California Cable Television Association;
(14) A designee of the Motion Picture Association of America;
(15) A designee of the California Communications Association (CalCom);
(16) A representative of the California Banking Industry;
(17) A representative of the California Office of Information Security and Privacy Protection;
(18) A representative of the California Department of Finance;
(19) A representative of the State Chief Information Officer;
(20) A designee of the Recording Industry of America; and
(21) A designee of the Consumers Union.

Section 2.
The chairperson of the Committee shall be selected by the Executive Director of the Office of Emergency Services from among the members of the Committee [Penal Code Section 13848.6(d)].

ARTICLE III: POWERS AND DUTIES

Section 1.
The Committee is empowered to act as the advisory board of the Office of Emergency Services in accordance with the mandates of the pertinent state acts and programs. The Committee may develop and/or modify and recommend to the Office of Emergency Services a high technology plan.

Section 2.
The Committee may develop policy recommendations for the Governor, the Legislature, the Office of Emergency Services and the local units of government on major criminal justice issues where a high technology nexus exists. To that end, the Committee understands itself to be the primary advisory board on technology-related criminal justice issues.

Its goals include:
1. Identifying current, developing and future issues involving high technology crime and criminal justice policy and procedures relevant to such issues;
2. Developing an understanding of the issues attendant to high technology crime and making conclusions that provide the foundation for recommendations to the Office of Emergency Services, the Governor and the Legislature concerning high technology crime, criminal identification, apprehension and prosecution;
3. Issuing analysis of current or pending high technology criminal justice-related legislation;
4. Assisting California's criminal justice agencies and practitioners in the effective use of resources regarding high technology crime;
5. Coordinating studies and recommendations with the Office of Emergency Services and other criminal justice agencies with a view toward isolating issues common to high technology crime and justice.

ARTICLE IV: COMMITTEE MEETINGS

Section 1.
The Committee shall meet at such intervals as necessary to carry out its duties, but no more than twelve meetings shall be held annually. Regular meetings of the Committee shall be held at least quarterly unless, in the opinion of the Committee Chair and Vice Chair, there are insufficient items of business or insufficient funds to call such quarterly or regular meetings. The Executive Secretary of the Committee shall give a minimum of ten days written advance notice to the membership of the Committee of the time and place of a regular meeting.

Section 2.
Special meetings of the Committee may be called at any time by the Committee Chair. Forty-eight hours prior notice of the time and place of such special meetings shall be given by the Chair to the members, where permitted by law.

Section 3.
Meetings shall be conducted in accordance with these bylaws and Robert's Rules of Order.

ARTICLE V: SUBCOMMITTEES AND SUBCOMMITTEE MEETINGS

Section 1.
The Committee shall have the following subcommittees:

--Strategy Subcommittee
--Bylaws Subcommittee

ARTICLE VI:

Section 2.
The Committee may recommend the creation of such subcommittees of its own membership as it deems necessary.

Section 3.
By a majority decision, the Committee may request the review of any subcommittee's decisions or activities.

Section 4.
Each subcommittee of the Committee shall meet as often as the subcommittee members find to be necessary.

Section 5.
All subcommittees shall be ad hoc in nature, and sit at the pleasure of the Committee Chair and a majority vote of the membership present at the time of the subcommittee creation.

ARTICLE VII: OFFICERS AND DUTIES

Section 1.
The officers of the Committee shall be the Chairperson (Chair) and the Vice Chairperson (Vice Chair).

Section 2.
The Chairperson shall be chosen by the Executive Director of the Office of Emergency Services from among members of the Committee, and shall serve at the pleasure of the Director. The Vice Chair shall be chosen by the membership of the Committee from among members of the Committee.

Section 3.
The Chair shall preside over all meetings of the Committee, and perform such additional duties as requested by the Committee and normally executed by a chairperson. The Chair shall create such standing and ad hoc committees as are deemed necessary to carry out the powers, duties and mission of the Committee. The Chair also shall appoint all members to both standing and ad hoc committees. All such subcommittee members shall serve at the pleasure of the Chair.

Section 4.
In the absence of the Chair, the Vice Chair shall preside at meetings and perform such additional duties as are required by the Committee and necessitated by the absence of the Chair.

Section 5.
In the event a vacancy occurs in the office of the Chairperson, the Director shall designate a successor prior to the next regular or special meeting. In the event a vacancy occurs in the office of the Vice Chairperson, the membership of the Committee shall designate a successor at the next regular or special meeting (Penal Code 13810).

ARTICLE VIII: QUORUM, VOTING AND ATTENDANCE

Section 1.
A quorum of the Committee for any meeting shall consist of a majority of the members designated or appointed at the time of the meeting. If a quorum is present, a majority vote of the members present is necessary for Committee action, except for the suspension of these bylaws pursuant to Article XII.

Section 2.
No vote by an alternate will be honored except as provided for in this section.
a) An alternate designation letter is required from any absent Committee member, and shall be presented to the Committee prior to the start of the next regular or special meeting.
b) An alternate will have full voting rights, floor rights, and be included in quorum determinations.
c) Alternated attendance for a Committee member will negate provision of Section 3 below.

Section 3.
Any member of the Committee who misses three consecutive meetings or who attends less than fifty percent of the Committee's regularly called meetings during one calendar year shall be automatically removed from the Committee, except in situations in which the Chair finds that such deficiency is the result of illness or injury.

ARTICLE IX: REIMBURSEMENT OF EXPENSES

Section 1.
Members of the Committee shall not receive compensation for their services but will be reimbursed for those actual and necessary expenses incurred which relate to their duties as Committee members.

Section 2.
Members of continuing task forces, review committees or of any other Committee-established auxiliary bodies who are not Committee members shall not receive compensation for expenses, unless prior approval has been obtained from the Office of Emergency Services. However, individuals who appear before the Committee at its request in order to review specific topics on one or more occasions shall be reimbursed for their necessary travel expenses.

ARTICLE X: EXECUTIVE SECRETARY

Section 1.
The Executive Secretary of the Committee shall be appointed by the Director of the Office of Emergency Services

Section 2.
The duties of the Executive Secretary to the Committee shall be to provide staff support to the Committee including keeping all records, preparing agendas for each meeting, keeping minutes and approving all Committee expenditures.

Section 3.
The Executive Secretary shall, in accordance with applicable law, be responsible for any additional staffing, planning, organizing, coordinating, and directing to those activities necessary to assure the fulfillment of the powers, duties, and mission of the Committee.

ARTICLE XI: CONFLICT OF INTEREST

Section 1.
No member of the Committee shall participate personally through decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise in any proceeding, application, request for a ruling or other determination, contract, grant claim controversy, or other particular matter in which funds under jurisdiction of the Committee are used, where to his or her knowledge he or she or his or her immediate family, partners, organization other than a public agency in which he or she is serving is an officer, director, trustee, partner, or employee or any person or organization with who he or she is negotiating or has any arrangement concerning prospective employment, has a financial interest.

Section 2.

In the review of proposals under appeal before the Committee, members of the Committee shall avoid any action which might result in, or create the appearance of:
a) Using his or her official position for private gain
b) Giving preferential treatment to any person
c) Losing complete independence or impartiality
d) Making an official decision outside official channels
e) Affecting adversely the confidence of the public in the integrity of the Government or the program.

ARTICLE XII: AMENDMENTS TO THE BYLAWS

Section 1.
Amendments

HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE

MEMBERSHIP ROSTER

MEMBER/ADDRESS/TELEPHONE	ORGANIZATION REPRESENTED
William E. Eyres – Chair 8831 Berta Ridge Court Prunedale, CA 93907 831-663-3695 eyres@montereybay.com	**Appointed by the California Emergency Management Agency (Cal EMA)**
Saul Arnold – Vice Chair Corporate Counsel, Legal Services Law Department Applied Materials, Inc. 3050 Bowers Ave. M/S 2062 P.O. Box 58039 Santa Clara, CA 95054 408-563-4590 408-986-2836 (fax) saul_arnold@amat.com	**Semiconductor Equipment and Materials International**
Janette Gunther-Allen Special Agent in Charge California Department of Justice Bureau of Investigation and Intelligence 3046 Prospect Park Drive, Suite #1 Rancho Cordova, CA 95670 916-464-3640 916-825-7576 (fax) janette.guntherallen@doj.ca.gov	**California Attorney General's Office**
~~**Mark Weatherford**~~ **NEW APPT NEEDED** ~~Chief Information Security Officer~~ ~~California Office of Information Security~~ ~~1325 J Street, Suite #1650~~ ~~Sacramento, CA 95814~~ ~~916-323-7322~~ ~~mark.weatherford@oispp.ca.gov~~	**State Chief Information Officer**

Troy Abney — **California Highway Patrol**
Assistant Chief
Information Management Division
California Highway Patrol
601 North 7th Street, Building C
Sacramento, CA 95811
916-843-4000
tabney@chp.ca.gov

Jack Christin, Jr. — **California Internet Industry**
Associate General Counsel — **E-Bay/PayPal**
eBay, Inc.
2145 Hamilton Avenue
San Jose, CA 95125
408-376-5145
408-376-7517 (fax)
jchristin@ebay.com

Mark Domnauer — **American Electronic Association**
Director, Global Safety and Security — (California Computer Software Producers)
Adobe Systems Incorporated
345 Park Avenue, MS A09-406
San Jose, CA 95110
408-536-4049
408-536-6616 (fax)
domnauer@adobe.com

Joseph Ford — **California Banking Industry**
SVP and Chief Security Officer
Bank of the West
180 Montgomery Street, 4th Floor
San Francisco, CA 94104
415-765-4877
415-399-7233 (fax)
joseph.ford@bankofthewest.com

~~**Merle (Bud) Frank**~~ **NEW APPT NEEDED** — **California District Attorneys Association**
~~Deputy District Attorney~~
~~County of Santa Clara~~
~~County Government Center, West Wing~~
~~70 West Hedding Street~~
~~San Jose, CA 95110~~
~~408-792-2469~~
~~408-279-8742 (fax)~~
~~Bfrank@da.sccgov.org~~

~~**Margaret Felts**~~ **NEW APPT NEEDED** **California Communications Association (CalCom)**
~~President, California Communications Association~~
~~1321 Howe Avenue, Suite 201~~
~~Sacramento, CA 95825~~
~~916-567-6702~~
~~916-922-3648 (fax)~~
~~mcf@calcom.ws~~

Brian Gurwitz **Recording Industry Association of America**
Law Office of Brian Gurwitz, APC
1422 Edinger Avenue, Suite 100
Tustin, CA 92780
714-880-8800
714-880-8801 (fax)
Brian@Gurwitzlaw.com

James Cooper **California State Sheriff's Association**
Captain
Sacramento County Sheriff's Office
PO Box 214327
Sacramento, CA 95821
916-874-3007
jcooper@sacsheriff.com

Steven Lund **American Electronic Association**
Director, Corporate Security (California Computer System Manufacturers)
Intel Corporation
4500 S. Dobson Road, OC4-35
Chandler, AZ 85248
480-715-5036
Steven.j.lund@intel.com

Jason Moore **California Cable & Telecommunications Association**
Regional Director of Security
Comcast Cable
3055 Comcast Place
Livermore, CA 94551
925-424-0384
Jason_Moore@cable.comcast.com

John McMullen, Lieutenant (Retired) **High Technology Crime Investigation Association**
Santa Clara County District Attorney's Office
Bureau of Investigation
PO Box 620158
Woodside, CA 94062
650-722-1877 (cell)
inspector19@mac.com

Joanne McNabb
Chief, California Office of Privacy Protection
California Office of Information & Privacy Protection
915 Capitol Mall, Suite 200
Sacramento, CA 95814
916-651-1057
916-653-3815 (fax)
Joanne.mcnabb@scsa.ca.gov

California Office of Information & Privacy Protection

Bruce Muramoto
Chief of Police
City of Winters
318-A First Street
Winters, CA 95694
530-795-2261 (ext. 121)
530-795-3921 (fax)
Bruce.muramoto@winterspolice.org

California Police Chiefs Association

Jennifer Osborn
Principal Program Budget Analyst
Department of Finance
915 L Street
Sacramento, CA 95814
916-445-8913
916-327-0225 (fax)
Jennifer.osborn@dof.ca.gov

California Department of Finance

Kevin Suh
Vice President
15301 Ventura Blvd., Building E
Sherman Oaks, CA 91403
818-935-5859
818-285-4408 (fax)
kevin_suh@mpaa.org

Motion Picture Association of America

Voluntary Vacancy

CTIA – The Wireless Association

Voluntary Vacancy

Consumers Union