International Association of Investigative Locksmiths

PROFESSIONALISM ~ TRAINING ~ EDUCATION

1507 Whitmarsh Circle, Severn, Maryland, 21144
1-800-598-9491 www.iail.org
WE SET THE INDUSTRY STANDARDS

Dewey, Cheatum & Howe

*"Can transponder equipped vehicles be stolen? Of course. The question isn't **IF** they can be stolen, but **HOW**! Hiring properly trained and equipped forensic locksmith/examiners is critical to an insurance company's proper evaluation of automotive theft." TGS*

by Tom Seroogy, CFL

Well, there's no doubt that Brad Stone has hit a nerve in his recent WIRED article "Pinch My Ride."

I normally don't have much interest, much less the time, for responding to articles regarding auto theft. In most instances, they are one-side and obtuse; filled with more rhetoric than fact; contrived by a writer trying to sell a point of view rather than exposing newly learned fact. However, in this case, the response by clients and colleagues was so overwhelming that it was necessary to address their concerns regarding statements issued as fact.

In reading Stone's article several items should be addressed including many credibility issues. For the sake of brevity, however, this article covers the three primary concerns: 1.) Stone's credibility, 2.) the problems with interpreting and evaluating the effectiveness of transponder-based security, and 3.) the credibility of the techniques, tools and methods which are mentioned in the article.

The STONE Credibility

Applying one of the most widely used themes and techniques in writing, Stone immediately stages auto theft as a battle of David v. Goliath. Assuming the role of David, Stone assigns the role of the detestable Goliath to the insurance companies and police. Then armed with the stories of spurned claimants, he quickly attempts to present himself as being fair and impartial by coloring the claimants as helpless victims of a merciless giant that seeks only its own best interest.

Stone builds on the Goliath image by portraying the insurance companies as being unresponsive to claimants and unwilling to submit to his requests for a response to the claimants' cases. What Stone fails to state, however, is that a company (ANY COMPANY) cannot legally or ethically respond to such requests. In other words, both the insurance companies and police are held out as the bad guy by following the very laws that protect the privacy of the individual claimant.

Reading further, Stone reveals the real motive behind this article – his own experience with auto theft. couched within the rhetorically heartfelt story of the theft of his own vehicle – endearingly referred to as "Honky" – Stone displays his distrust and disdain for insurance companies and police. In essence, Stone shows his hand - he has a score to settle.

Still, Stone should not be held wholly accountable for his view.

First, he is not an auto theft expert and is acquainted with only a pinhole view of the bigger auto theft-police-insurance picture, and an even smaller view of transponder-based security.

Second, his sweeping and over-generalized conclusions are based on the words of a few individuals who are portrayed as experts of transponder-based vehicle security. Stone is careful to craft their responses to present his perspective of transponder-based vehicle theft, carefully using portions of direct quotes that best reflect and reinforce his perspective. Lost are the direction of the questioning and the context of the answers.

Thirdly, it is a normal response for a person who has had a bad experience with an insurance company and/or police that may rely on forensic examiners that are not fully qualified or equipped to work with the constantly evolving transponder-based security found on today's vehicle's.

Finally, for Stone, writing is his livelihood. His success is fully dependent on his ability to draw the world's attention to the publication for which he writes. In the competitive world of written and web media, getting a reader's attention means that every story must have a hook – a device or angle that draws the reader to the story. This is most often accomplished at the expense of truth and objectivity.

Drawing a crowd worked in Stone's case. His one-sided, myopic and biased rendition on the theft of transponder-based vehicles apparently has the insurance world choking. So goes the power of the pen when you have an axe to grind. Stone may have raised the awareness of theft of high-tech vehicles, but not without inciting unjust and undue public disdain for insurance companies, police, and forensic locksmiths/examiners through the use of broad and sweeping conclusions based on minimal and sometimes misleading information.

Problems with INTERPRETING & EVALUATING Transponder Technology

While Stone's conclusions regarding methods of theft of transponder-based vehicles are skewed, he does bring to light several very important and key issues – the misplaced trust, or should I say "faith", in the integrity of transponder-based immobilizer systems, the competency and training of those evaluating transponder equipped vehicles, and the fact that methods of theft evolve directly behind changes in technology. For these he should be commended.

Before we address the concerns regarding the various methods of transponder-based vehicle theft mentioned in his article, however, we need to understand some of the reasons for the diversity of opinion and error in understanding and evaluating theft of automobiles equipped with transponder-based anti-theft systems. Factors affecting our understanding of transponder technology include the creation and propagation of Myths & Urban Legends, the use of the Internet, Chronology, and the Multifarious Nature of the systems.

MYTHS & URBAN LEGENDS

The term Myth is not meant to be demeaning, but rather to reveal the basic nature of people to over-generalize or impose a certain perspective or belief of a given situation or condition to answer or account for things not yet understood.

While many myths have their root in truth, the conditions required for the cause-effect process that originally formed the basis of the myth are often overlooked or not understood. Eventually, over time and despite changes in conditions, a known cause is often attributed to a known effect without true evaluation as to their relationship. Soon speculation and supposition replace detailed analysis and employment of the scientific method, eventually resulting in unsubstantiated statements of fact and incongruency in the cause-effect relationship.

One myth and one event serve as perfect examples.

First the myth. Jumping relays has long been promoted as a means of bypassing a vehicle's transponder system. Self-proclaimed experts have been demonstrating this technique for years. Inferred through their demonstration is that relay jumping can be applied to all years, makes, and models of vehicles equipped with transponder security. What these experts don't reveal are the limitations of this technique. More on this technique is covered later in this article.

Next, the birth of a myth. A photograph of a small device attached near the handle of a late model Prius was distributed via email with a request to identify the component. The attached message stated that moving the device caused the Prius door to lock and unlock.

Needless to say, there was an outpouring of speculation as to the type and operation of the unidentified device. Answers ranged from simple disbelief that the device had any affect to spectacular conjectures that the device intercepted and trapped the radio signals of the Prius transmitter.

Taking the bull by the horns, one experienced forensic locksmith contacted the originator of the message and asked a few questions. The questions were followed up by another examination of the device and its operation. In short, it was found that during the original exam, the owner with transmitter in hand had been in close proximity to the vehicle. After moving the transmitter away from the vehicle, the device had no affect on the vehicle. It was learned that it was this transmitter and not the unidentified device that initially caused the Prius door to lock and unlock.

Although the device is not yet officially identified, it appears to be nothing more than a contact microphone. Still, due in part to the nature of the internet, many are still under the belief that it was the device that operated the vehicle door lock. The beginnings of a myth.

The INTERNET

The anonymity and ubiquitous reach offered by the internet creates several problems in addressing transponder technology and auto theft. The first is its ability to propagate myths and urban legends, allowing them to sprout up overnight. Unfortunately, the dissemination of incorrect or incomplete information makes it very difficult for even the most experienced expert to discern, separate, test, and prove a purported fact. One of the hardest tasks of a forensic examiner today – especially those involved in today's vehicle theft – is separating fact from fiction and effectively relaying it to a client and/or a jury.

Secondly, the internet and web create a venue for further impeding auto manufacturer, law enforcement, and insurance company efforts to control theft. Once a method for bypassing a vehicle's anti-theft system is discovered, the web has proven to be a powerful tool for broadcasting the information to the general public where it can be accessed by those wishing to take advantage of such techniques and methods for illegal purposes.

CHRONOLOGY

As Stone rightly states, the introduction of new technology is quickly followed by ways to bypass such technology. What is missing in Stone's analysis of the various methods – as well as that of many self-proclaimed or inexperienced experts – is the chronology of specific systems and the methods and techniques used to bypass them. In the timelessness of the internet, methods of theft often appear to exist simultaneously with the introduction of a new technology. More frequently, a method of bypassing a system is incorrectly applied to systems several generations older than the ones they truly bypass. Stone indicates that systems are often only good for a couple of years. While true for some systems, many are robust and scalable enough to stand for many years; allowing for evolutionary changes that keep them secure for years to come. Still, the issue is not necessarily how long a system lasts, buy rather which ones do or do not last. Unfortunately, Stone's analysis is applied across all transponder systems regardless of accuracy.

When applied to forensic analysis, knowledge of a specific system's timeline and the tools and methods (both legal and illegal) available for bypassing it are critical. In one case, an insurance company paid the claim on a 2001 Audi A6 based on a forensic locksmith's report that a "black box" existed allowing the bypass of the vehicle's transponder system by connecting directly to the OBDII port. In reality, while a device existed for bypassing some VW and Audi vehicles, it did not work on the systems employed in North American models at the time of the theft.

Other methods subject to the timeline errors include fallacies regarding the ability to swap modules or clone keys to affect the theft of a transponder equipped vehicle.

The MULTIFARIOUS NATURE of Transponder Systems

Probably the most common reason for error is the lack of knowledge regarding the intricacies of the various

transponder systems. For simplicity's sake, transponder systems are often explained and defined in broad, generalized terms. While this may be good for those beginning to understand transponder security and needed when trying to explain to the public at-large; it hardly fits the specialized needs of auto theft.

Like any evidence, transponder systems have both class and individual characteristics. While many forensic examiners, law enforcement officers, and insurance SIU personnel are familiar with the class characteristics, most are not familiar with the intricacies of the individual characteristics. Yet it is these characteristics that have the greatest effect on one's findings.

For example, on a late model Ford, given one properly cut and programmed key submitted for examination and a diagnostic test indicating that two keys are programmed into the vehicle, an experienced forensic locksmith/examiner is able to make a conclusion regarding the status of the two keys programmed into the vehicle and the one submitted for examination. Likewise, a single key known to start and operate a late model Nissan offers information strategically significant to status of all the keys used on this vehicle.

Credibility of TOOLS, TECHNIQUES & METHODS

Before covering the various methods of theft that Stone raises, one needs to understand that no person is beyond being able to commit insurance fraud. Every day, police officers, firemen, and insurance companies are faced with the fact that insurance fraud is an equal opportunity employer. Men and women, the elderly and teenagers, husbands and fathers, wives and mothers, wealthy and poor, movie stars and the homeless, police officers and firemen, pastors and laymen; history tells us that all groups are capable committing fraud by staging a theft of their automobile. For some, the reasons are easily recognized – debt, divorce, or other personal and catastrophic problems. For others, it's simply an acceptable method of benefiting at the expense of that cold Goliath – the insurance company.

In one solved case, a couple admitted to staging a theft and arson of their vehicle. From the start forensic examination indicated no other way for the reported theft to have occurred. There appeared to be no motive. The couple had no money problems. The car was well within their known budget. There were no family problems or conditions that would precipitate such a crime. Finally admitting to the fraud, the reason was revealed. They didn't like the color of the vehicle.

CASE – Emad Wassef, 2003 Lincoln Navigator

Stone reveals only a small bit of a larger picture in evaluating this specific theft/fraud. The system in the 2003 Lincoln Navigator is a fairly robust system. There are currently no commercially available tools that allow cloning of the keys (although one is due out in September. Go to www.vinlocksmiths.com for more information). Further, the bypassed ignition infers that a key was not present.

Relay jumping is not practical on this vehicle. Fuel-air supply and other essential engine functions are controlled by the PCM for which relay jumping does not work.

Vehicle diagnostics are critical to evaluating how a vehicle may have last been operated. This data is not provided by Stone. A qualified forensic locksmith/examiner, armed with the correct tools and experience, can retrieve data from the vehicle that provides clues as to the status of the vehicle at the time of last operation. This data may have been provided to the insurance company – but not to the general public.

Although aftermarket and Ford factory tools are available for programming these vehicles, none currently bypass the manufacturer's security scheme for programming keys into them. Does this mean that they cannot be used? Hardly, however, this probability of using such a tool for theft is dictated by the circumstances of the theft (time, location, etc.), and outside the scope of a forensic locksmith/examiner's exam. In some instances, data can be retrieved confirming the use of such a tool. However, this requires the use of a forensic locksmith/examiner who is properly trained and experienced in this technology.

CASE – Ford Relay Jumping

"'The carmakers are calling these passive antitheft systems, but they're not,' says Rob Painter, a Milwaukee-based forensic locksmith who has testified in dozens of auto insurance court cases, for both sides. 'They are just theft deterrents. Tell me a car can't be stolen and I'll show you how to do it.'"

"By 2000, forensic locksmiths like Painter were demonstrating for juries how crooks were getting past the transponders in Fords: Pop the hood and pull a certain fuse from the power relay center in the upper left corner. Zap, you're in."

Known more for his verbal hyperbole than his substance and technical prowess, Painter has used this "trick" to infer that all Fords are easy to bypass. This method was developed and known long before Painter adapted it to his own purposes.

In short, this trick worked on early model Fords, most working off of the PATS system. Testing by this writer shows that both PATS I and PATS II vehicles may be vulnerable, typically those years covering Fords up through 1999. While commonly used on the truck/SUV line, it may extend to some sedans and passenger vehicles as well. Further, this technique must be accomplished within 10 minutes of the last operation of the vehicle. Ten minutes after the vehicle is turned off the PATS and PCM modules shut down and relay jumping does not work - a fact many experts fail to state.

Ford systems subsequent to 1999 are generally not prone to relay jumping, and those Fords starting with the use of the encrypted wedge transponder and movement of the key functions into the PCM are not susceptible to the relay attack.

A qualified and experienced forensic locksmith/examiner is able to determine whether the relay has been jumped. For video presentation of this in operation on a 1998 Ford Expedition go to www.vinlocksmiths.com.

CASE – Pass-Key I and II

"The high lasted only a few years. People started complaining about not being able to replace lost keys easily, so GM opened a back door. Dealers and locksmiths got permission to stock key blanks, and by the early '90s police were arresting car thieves who had rings of all 15 GM keys."

Commonly referred to as VATS, carrying a ring of 15 GM Pass-Keys does not indicate the use of these keys for theft. First, the key has to be correctly cut. Second, the VATS value needs to be known. This was possible until recently, as key codes and VATS values were available via GM roadside assistance and authorized GM dealers.

If a value is not known prior to making a key, programming is completed by trying each key value separately. A four-minute delay is required between each attempt. In essence, key programming may take as little as 4 minutes and as long as one hour. The 1991 Corvette incorporated a programming sequence that increased the time delay after three unsuccessful attempts at programming. Where key codes and VATS values are not available, other destructive methods of bypass were possible.

Only a few electronic signatures exist for this type of system. Currently, GM does not make this information available except through authorized dealers. While use of a key as the last method of operation may be easily determined, how the key was obtained or created requires examination beyond the car.

CASE – Programming Equipment

"Meanwhile, transponder-equipped cars were being resold to new owners, and keys were disappearing behind couch cushions. Auto-repair supply and locksmithing companies started selling devices like the Code-Seeker and the T-Code, which allow anyone to create a new set of keys for a fixed-code transponder-equipped car. The Jet Smart Clone (catchphrase: "Clone the uncloneable!") duplicates any fixed-code RFID chip by reading its code and imprinting it onto the blank chip of a new key with the same mechanical cut."

Tools for programming and cloning transponder equipped vehicles have been available for some time. Early in their production, auto manufacturers, including Honda, denied the existence of these tools, insisting that their cars were, in fact, more secure than any others. These tools are capable of bypassing the key programming security scheme of many vehicles, typically those requiring PIN numbers. However, use of these tools often leaves signature indicators that a qualified and experienced forensic locksmith/examiner can use to determine their use.

CASE – Human Error

"Bay Area Mercedes lot in Pleasanton. A $78,000 black S430 disappeared overnight; police traced the car's GPS unit to the parking lot of a Fry's Electronics, but when they arrived at the store, they found not the missing Pleasanton car but another S430 stolen from a Monterey car lot earlier that year. They also found its driver, a 25-year-old San Jose man named Naheed Hamed.

"...inside the car, mechanics discovered a technological treasure trove: an original Mercedes electronic ignition system and custom Mercedes fuses, all wired with alligator clips to the dashboard and to the fuse box underneath the driver's seat. The car also held a Pelican PDA carrying case and a wireless RFID-signal-sniffing antenna. Investigators suspect that Hamed spliced in his own ignition system and power source, then used the PDA to upload pirated software to the car's computer to disable the transponder and swap the two cars' GPS tracking numbers. Of course, he also believed he could beat the cops in a car chase."

Human error and not transponder bypass is the cause of this theft. Once a vehicle is stolen, taking it to a garage for modification is not uncommon. The tools, programming equipment and information needed to make vehicle changes as listed above are available via internet channels.

More common among expensive, high-line cars like Mercedes and BMW, vehicles are often stolen, leased and even bought for transport overseas where the parts and systems are reverse-engineered.

Equipment and programs (sometimes pirated) are created and sold through backdoor markets, often for illegal purposes. Typically, this equipment is expensive, hard to locate, and harder to learn to use. Although typically used by organized crime, many of the less sophisticated tools were recently introduced for use into the locksmith market. The use of such equipment on a recovered vehicle is typically detectable.

CASE – Technology & Jiggle Keys

"That kind of technology is too expensive and too complicated for your basic chop-shop crew, but they usually don't need it anyway. For the past few years, Bay Area cops have pursued a ring of thieves that break into Hondas and Acuras with "jiggle" keys – keys with the teeth shaved down so they can turn the tumblers inside any car's door lock. After the thieves gain access, they shuffle through the glove compartment and snatch the manual, where dealers – unbeknownst to many car owners – often leave an extra valet key."

Like any business, chop-shops are going to do whatever it takes to reduce their costs, time and exposure to being caught. As technology advances, the price of the tools declines. Add to this end, the market for stolen tools, and the availability and use of programming tools to and by the "basic chop-shop" is simply a matter of time. Use of these tools to effect a theft is often detectable by a qualified and experienced forensic locksmith/examiner.

Jiggler keys (rocker picks, pick-keys, etc.) are not uncommon tools for entry and sometimes operation of a vehicle. However, the use of these tools leaves distinguishing marks that are easily discovered through good forensic work.

The "valet key in the glove box" is a common statement offered by victims of auto theft. A few manufacturers, including Lexus, made a practice of placing a spare key in the glove box, a practice they have since stopped.

This writer is currently in the process of research into methods and tools that allow examiners to query a vehicle for keys programmed into its system and allowing a full accounting and matching of known keys. Although moving through peer review by the International Association of Investigative Locksmiths (IAIL), this technique has already been used to vindicate the complicity of the insured in a reported theft. As the technology completes peer review, it is expected to be able to satisfactorily infer an insured's involvement and culpability in a reported theft. Several manufacturers now include a short "audit" of what keys were used in a vehicle and when. A properly equipped and trained forensic locksmith/examiner is capable of collecting and interpreting this data.

CASE – Transponder Vehicles Can Be Stolen

"Ivan Blackman, the manager of the Vehicle Information and Identification Program for the NICB, says that insiders are gradually getting over their dogmatic belief in the invincibility of transponder systems. "Companies are slowly realizing that the cars can be stolen," Blackman says."

Mr. Blackman is absolutely correct. Since the introduction of the first aftermarket transponder programming tool, this writer has been advising vehicle manufacturers and law enforcement of the various methods and

tools available for circumventing transponder-based security systems.

Most of the "dogmatic belief in the invincibility of transponder systems," came from a lack of knowledge of these systems and how they operated. This impression was further reinforced by forensic examiners who lacked the proper training and tools to understand and determine the class or individual characteristics of the various systems.

Countering this groundswell of "faith" in the invincibility of the transponder system were (are) individuals that were (are) equally untrained and inexperienced in transponder security, making ludicrous and obtuse claims like "Tell me a car can't be stolen and I'll show you how to do it."

Even today, insurance companies and examiners tend to sit on either end of the transponder spectrum. Again, this is due to lack of knowledge, training and experience with these systems.

CASE - 2003 Honda Civic or "Honky" Part I

"…The ignition cylinder was intact, and our keys still worked.

"I still didn't know what happened to Honky. Maybe someone at the dealership or a valet had cloned my key with a device like a Jet Smart Clone, then showed up later to take the car. It was also conceivable that someone grabbed the vehicle identification number off the dash, went to the dealership, pretended to be me, and had an extra key produced. Still, either scenario seemed like it would require an awful lot of footwork for a Pantera- and nicotine-fueled joyride."

Cloning requires a targeted theft. This is realistic, but usually occurs on a limited demographic basis. Targeting involves a degree of organization and access to tools by the perpetrator. And, unfortunately, determining such a theft requires good police work in examining patterns in vehicle theft from their jurisdiction.

CASE – 2003 Honda Civic or "Honky" Part II

"Then I heard about another possibility. Earl Hyser, the superintendant of State Farm Insurance's Vehicle Research Facility, told me that some transponder-equipped cars came with a secret "cheat" code designed to allow people who lose their keys to drive back to the shop. I asked the SFPD about it and was referred to Ken Montes, famous in Bay Area street racing circles for a souped-up 1992 Honda Civic…

"…I walked outside and approached Honky. The door lock would have been easy – a thief would have used a jiggle key, and a stranded motorist would have had a locksmith cut a fresh one. I just wrapped the grip of my key in tinfoil to jam the transponder. The key still fit, but it no longer started the car.

"Then I grabbed the emergency brake handle between the front seats and performed the specific series of pumps, interspersed with rotations of the ignition between the On and Start positions. After my second attempt, Honky's hybrid engine awoke with its customary whisper."

Interestingly, Stone used the rather emotionally charged term "cheat" to describe Honda's Emergency Brake Code. While quoting Mr. Hyser of State Farm Insurance, the term is probably used out of context. This feature of the Honda/Acura vehicle has been known by the writer since Honda's release of its first transponder equipped vehicle, and is often demonstrated to tactical automotive law enforcement agents.

With respect to the "cheat" codes, there are currently only two manufacturers (Honda/Acura and Mitsubishi) that employ them. These codes are used to allow the vehicle to be started and driven should the keys be lost. In short, when a key is lost, a mechanical key must be made, the BRAKE code obtained from an authorized Honda dealer, and the BRAKE code procedure performed on the vehicle. The BRAKE code procedure must be repeated after every instance where the vehicle is turned OFF for more than 10 minutes.

While Stone quite correctly shows how this method can be used to steal a Honda car, there is an inference that this is a common method for theft. Like cloning keys, however, in all probability, this occurs on a demographically local basis. Honda dealers are the only source for the BRAKE codes and typically do not divulge them without prior proof of ownership. Thus, illegitimate use of the Emergency Brake code requires involvement through a source at an authorized Honda dealer, and is a targeted theft. Again, while this is not unrealistic, it may require a number of similar thefts and some good detective work to determine that such a pattern exists.

CONCLUSION

Overall, Stone's negative experience with the police and insurance company although regretful, is not the result of unwarranted and prejudicial treatment by these agencies. Daily immersed in cases of fraud committed by the most unlikely perpetrators, police officers, arson investigators, and SIU personnel develop a wary eye for any reported theft. This is especially true when there appears to be no indication of bypass to the vehicle's mechanical or electronic security.

Likewise, bypassing a vehicle's security features is only a small piece of the overall auto theft fraud puzzle. Motive and opportunity are integral to making a conclusion as to whether a car was legitimately stolen or if there was owner involvement. An SIU cannot make these determinations based solely on how a vehicle was last operated.

Further, there are self-proclaimed forensic examiners who claim they can determine whether or not a car was stolen. This is wholly ludicrous. A properly trained examiner may be able to determine how the vehicle was last operated or even moved (in the case of towing or lifting). What a forensic automotive locksmith/examiner cannot tell you is the people involved or the motive behind the incident. In other words, an examiner can tell you the "how," but not "who" or "why." This is the responsibility of the police and specially trained insurance investigators.

Thus forms the basis for the perpetual dilemma of the relationship between police/insurance company and the general community; it is this victim-accused quandary that I believe is at the root of Stone's rather vitriolic article. Based on what Stone revealed of "Honky's" theft, the pattern probably suggests some owner involvement. And, while the insurance company and police may have left him feeling like a suspect and not a victim, it is probably the research of these very agencies that prevented them from pursuing criminal fraud charges. On the other hand, this does not excuse either the police or insurance company for offensive or accusatorial behavior. While fraud is a very difficult offense to detect and pursue, offending the very people you're paid to protect doesn't bode well for public opinion of the police department or insurance companies.

Realistically, Stone properly concludes that theft of a car equipped with a transponder-based immobilizer system is possible. However, to avoid unjust and undue accusations, police, insurance companies and individuals need forensic locksmith/examiners who are fully qualified to examine both mechanical and electronic security features of a vehicle. Independent and non-profit forensic organizations like the International Association of Investigative Locksmiths need to be tapped for examiners who are qualified and have the proper tools and resources for examining vehicle locks, keys, security systems (original equipment and aftermarket), as well as performing proper diagnostics on the vehicle's electronic system.

Thomas Seroogy, CFL

David Drew, CFL

Glenn Hennings CFL, CRL, RST

Ken Vitty, CRL, CFL, CFI

Robert Mangine, CFC, ACFEI, CFEI

Herbert T. Miller, CFL, CFEI, BCEP

Richard J. Pacheco, BCFE, CFEI, MFE, CFL
Master Forensic Examiner
Fellow, American College of Forensic Examiners
Diplomat, Board Certified Forensic Examiner
Independent Consultant

Stan Paluski, ASE Certified, Forensic Technician

Jonathan Costa
Forensic Analyst
ASE Certified Master Technician
Oil Filter Technician,

Liberal Oliveira, CFL, IL, CFII, CFEI
Senior Forensic Analyst
ASE Certified Technician
Certified RI Auto Inspector
Oil Filter Technician