Welcome to our fourth annual Stevenson University Forensics Journal. This year, as always, we bring fresh voices and perspectives from all aspects and areas of the field.

I am pleased to note that a new section has been added this year, highlighting the process of library research in the vast field of Forensic Studies. Our Stevenson University librarians bring the research process into the twenty-first century by showcasing a variety of on-line resources available to researchers.

Also of note is the connection between our cover photo and the interview conducted with Dr. David Fowler, Chief Medical Examiner for the State of Maryland. Assistant Editor Stephanie Witt joins the Journal as a contributor to explain the fascinating Nutshell Series of Unexplained Deaths.

We are privileged this year to have the Honorable Lynne A. Battaglia providing her insights into the Court’s perspective on the prominent role of forensic evidence in modern litigation. Judge Battaglia highlights the interrelationship between the law and science for forensic students and professionals.

I hope you enjoy and are enlightened by this edition of the Journal.

Carolyn Hess Johnson, Esquire
Editor and Publisher
Over the last few centuries, there have been numerous technological advancements in the field of forensics, death investigation, and law enforcement. However, none are as beautiful, yet disturbing as Francis Glessner Lee's creations titled, "The Nutshell Studies of Unexplained Death." Created in the 1930's and 1940's, these three dimensional models were used in training law enforcement to investigate crime scenes by methodically searching for and analyzing evidence on dollhouse sized dioramas. Depicted in the cover photograph is the nutshell titled, "Three Room Dwelling." This specific nutshell represents a bloody crime scene in which a man and woman are found dead in their bed room. The immense detail that Francis Glessner Lee incorporated into these nutshells is evident throughout the model. While these nutshells were created nearly seventy years ago, their message and value still hold relevance in the field of death investigation today.

FRANCIS GLESSNER LEE

Born in 1878 to a wealthy family, Francis Glessner Lee was blessed with a luxurious home life and elite social status (Ramsland). Her father, John Jacob Glessner, obtained his wealth from the agricultural machinery and equipment manufacturer, the International Harvester (Ramsland). Despite her high-class upbringing, domestic influence, and expectation to become a proper woman, Lee favored a more rewarding and accomplished life. Her interest in law and medicine developed at an early age; however, she was prohibited from pursuing higher education, as she was expected to uphold the family social status. She married attorney Belwett Lee in 1898, had three children, and eventually divorced in 1914 (Botz, 23). During this time, she continued to years for a more fulfilling and significant existence. Despite her strong passion to pursue an education and become involved with legal medicine, the expectations of her family hindered this path. Her interests turned more specifically to crime investigations as a result of her friendship with Harvard medical students, George Magrath. Hearing stories of true crime and complaints of inaccuracy in the assignment (Botz, 33). No detail was too insignificant and each required investigators to think critically about evidence found at a crime scene.

Not meant to serve as "whodunit" scenarios, these models were instead created to provide a deeper analysis of evidence found at a crime scene and the questions that should be asked by investigators to gain more information (Botz, 29). Circumstances in accidents, homicides, and suicides can parallel each other creating difficulty in differentiating the type of crime, especially if evidence found is taken at face value only. Evidence that may seem insignificant may provide deeper insight to the circumstances surrounding the crime. If reviewed carefully and in proper context, while evidence may appear exac tant upon first glance, it may in fact hold no importance if further investigated. The nutshells were developed in parts, mind. They included minute clues, which would require law enforcement officials to adopt an investigative mindset when analyzing a crime scene. For example, some of the nutshells incorporated evidence, which would be considered time or temperature sensitive (one nutshell included a package of raw meat, which if investigated, may give police a better idea of the time the crime occurred). These types of clues would give the investigators a path to follow, questions to ask, and evidence to investigate further.

Beginning in 1945, the nutshells became an integral part of the Harvard Seminars on Legal Medicine (Botz, 29). These seminars were held twice a year and allowed investigators the opportunity to try their hand at deciphering Lee’s creations. Bringing together experts from around the world, Lee was able to provide investigators with valuable training that would sharpen their investigative skills and could be applied to future cases. She was appointed a Captain by the New Hampshire State Police and was soon the first woman to join the International Association of Police Chiefs (Botz, 30). Her fortitude encouraged collaboration among law enforcement and medical examiners and assisted in developing the medical examiner system as it is known today.

At the time of Lee's death in 1962, she had created twenty of these crime scenes, however only eighteen remain intact today. They are still used to train police officers to investigate crime scenes while looking at the crime from a medical perspective. The nutshell models are currently housed in the Office of the Chief Medical Examiner’s Office in Baltimore Maryland. While not generally open to the public, the Nutshells are thoroughly referenced in Corinne May Botz's book, The Nutshell Studies of Unexplained Death. Botz's book provides a detailed look at Lee's legacy and the passion which drove her to create such captivating models which would ultimately bring attention to the field of medical investigation and ultimately influence its advancement for years to follow.

REFERENCES

CAROLYN HESS JOHNSON, ESQ. is an attorney and a full-time Professor of Forensic Studies in the School of Graduate and Professional Studies at Stevenson University. She has worked in private practice, as a Senior Assistant State Prosecutor for the State of Maryland and as an Assistant State’s Attorney in Baltimore City, Maryland.

ABIGAIL HOWELL edited technical proposals, award packages, and various studies for submission to the Secretary of the Navy, Chief of Naval Operations, and Secretary of Defense. Subject matter included: telecommunications systems management and innovations, combat systems maintenance, Occupational Safety and Health Administration compliance, environmental compliance and initiatives, installation management excellence, and base realignment and closure proposals. Adjudication experience includes cases pertaining to Uniform Code of Military Justice violations, combat-related disabilities, physical evaluation board determinations, and military discharge characterizations.

STEPHANIE WITT completed her undergraduate studies in 2008 at the University of Baltimore, with a B.S. degree in Forensic Science. She continued her studies at Stevenson University where she received a Master’s degree in Forensic Science in May 2011. Stephanie currently works at Stevenson University as the Assistant to the Dean in the School of Graduate and Professional Studies.

ABOUT THE COVER: THE NUTSHELL STUDIES OF UNEXPLAINED DEATH
STEPHANIE WITT

INTERVIEW WITH DAVID FOWLER, CHIEF MEDICAL EXAMINER FOR THE STATE OF MARYLAND
CAROLYN HESS JOHNSON, ESQUIRE

INTERVIEW WITH JUDGE LYNN BATTAGLIA, COURT OF APPEALS
SUE SCHENNING, ESQUIRE

APPROACHES TO LIBRARY RESEARCH IN FORENSICS
MAUREEN BECK AND SARAJ GODBEE

NOT SO FUNNY FUNNY-MONEY: THE THREAT OF NORTH KOREAN COUNTERFEITING U.S. CURRENCY
ERIC W. CORBETT

E-SCAMS: CATCHING FRAUDSTERS IN A TECHNICAL WORLD
KATHERINE MASSEY

IMPACT OF STEGANOGRAPHY ON A FORENSIC INVESTIGATION
RYAN SPISHOCK, CESP

ACCOUNTING CONTROLS FOR NONPROFIT RELIGIOUS GROUPS
ROBERT WILLEY

ARE YOU FUNDING TERRORISM? IDENTITY THEFT’S ROLE IN TERRORIST FINANCING & A COMPREHENSIVE APPROACH TO PREVENTION
PHILLIPA NASH

MICROSTAMPING: THE LAST FRONTIER IN FIREARM IDENTITY
ROCHEL BENJAMIN

A STICKY WICKET: TRANSFERRING PROTECTED DATA FROM THE EUROPEAN UNION TO COMPLY WITH THE FOREIGN CORRUPT PRACTICES ACT WITHOUT VIOLATING EUROPEAN PRIVACY LAWS
KATHY KIRKISH, CFE

FALLIBILITY ISSUES IN FORENSIC EVIDENCE
BROOKE BREVENIK

SKYPETM ARTIFACTS
KAREN LYNNE SHAFER
Interview with David Fowler, Chief Medical Examiner for the State of Maryland
Carolyn Hess Johnson, Esquire

Interview conducted on Thursday, January 17, 2013:

PLEASE TELL ME ABOUT YOUR EDUCATIONAL AND PROFESSIONAL BACKGROUND.

I grew up in Zimbabwe and did medical training at The University of Cape Town in South Africa. I did my internship in general medicine and general surgery followed by a year of pediatric pathology training. I then became interested in forensics and completed a five year training program in forensic pathology at the University of Cape Town as well. When I moved to the States I had to complete another four year residency prior to taking my Boards as required by the American Board of Pathology.

WHAT EDUCATION AND DEGREES ARE REQUIRED TO BECOME A MEDICAL EXAMINER?

A Medical Examiner must obtain a four year undergraduate degree as well as an M.D. (Doctor of Medicine) or D.O. (Doctor of Osteopathic Medicine) degree from a medical school. In addition, the candidate must complete a general pathology residency for five to four years after medical school. Also, an additional yearlong forensic pathology fellowship is required.

WHAT TYPE OF FIELD TRAINING OR HANDS-ON WORK IS REQUIRED TO BECOME AN ASSISTANT, DEPUTY AND/OR CHIEF MEDICAL EXAMINER?

The minimum training and experience for an assistant are the education and the residences. The position of Deputy Medical Examiner requires ten to five years of professional experience. To qualify for the position of Chief Medical Examiner, five to ten years of experience is required.

WHAT IS THE STRUCTURE, BOTH PHYSICAL AND ADMINISTRATIVE, OF THE MEDICAL EXAMINER’S OFFICE?

The Medical Examiner’s Office is independent and not under the control of any law enforcement agency. The Medical Examiner’s system grew out of an independent coroner system. In this way we remain unbiased. We operate out of a single central Medical Examiner’s office, in Baltimore City, which allows us the economy of scale because everything is in one building. In this way we can attest rounds together, discuss cases together and provide backup, consultation and support for each other on cases. Most cases are presented to all of the staff at least once or twice through the process, drawing on the collective experience of two hundred years of death investigation in this office. There are fifteen full time Medical Examiners working in this office.

WHAT ARE THE RESPONSIBILITIES OF THE MEDICAL EXAMINER’S OFFICE?

The overall charge of our office is to investigate deaths in Maryland. The Medical Examiner’s Office is responsible for any questionable death that occurs in the state of Maryland. A questionable death is defined by statute in Maryland as that which occurs as a result of violence, suicide, casualty (trauma or accident), a child born and then dying outside of a medical facility or dying in a suspicious or unusual manner. It is the suspicious and unusual term that allows us to get involved in the investigation. Every case is reviewed by a Medical Examiner. If a question remains after time, the Medical Examiner’s Office is permitted to enter the scene and conduct an investigation. When a death is determined to be suspicious, the case is then opened, and a Medical Examiner is assigned. We use a model that assigns cases to be worked by a Medical Examiner and their resident. Assignments are rotated between Medical Examiners, but if a Medical Examiner is unwilling to do a particular assignment, which can happen on occasion, there are others who are always willing to take over.

ARE THERE SPECIALISTS IN YOUR OFFICE OR DOES EACH MEDICAL EXAMINER PERFORM THE SAME TYPES OF DUTIES?

Although there are no special assignments given, there are Medical Examiners who have particular interests or specialties and will seek to participate in certain types of cases. Since we assign cases on a rotating basis, a Medical Examiner who is particularly interested in a certain type of work might work on a case alongside the assigned Medical Examiner.

WHAT IS A TYPICAL WEEK LIKE IN YOUR OFFICE?

In almost all cases the cause of death is determined, but manner of death is more complicated. Cause of death is determining what physiological, anatomic problem caused the death of the victim. Manner of death is determining how the death occurred. For example, a gunshot victim’s cause of death is a gunshot wound. That victim’s manner of death would then have to be determined as homicide, suicide or accident. Determining manner of death is based on more factors than just the autopsy and will include investigative information and the police report. The State’s Attorney and law enforcement will make determinations that may be different from ours. For example, we may call a homicide may be determined to be a justifiable homicide by the State’s Attorney’s Office and therefore no one is charged. Or, we consider an accident may be ruled otherwise by the police or the State’s Attorney’s Office.

WHAT IS THE MEDICAL EXAMINER REQUIRED TO MAKE THE DETERMINATION OF DEATH AND WHEN CAN IT BE MADE BY A DOCTOR OR OTHER MEDICAL PRACTITIONER?

Any non-natural death must be reported to the Office of the Chief Medical Examiner. If a doctor is willing to sign a death certificate at the scene, the victim will be transported to a funeral home and we will not become involved. In a situation where there is no doctor willing or able to sign a death certificate on scene, or there are suspicious or violent circumstances, the Medical Examiner must be called to the scene.

WHEN IS AN AUTOPSY REQUIRED?

This is determined by the Medical Examiner investigator at the scene who will interview witnesses, family members, speak to the police, review medical history and take any other circumstances into account. The investigator works with a Medical Examiner by phone to make the determination as to whether the body should be transported for an autopsy or the body will be transported to a funeral home and a death certificate can be signed by the Medical Examiner’s Office without an autopsy.

HOW OFTEN IS THE CAUSE OF DEATH UNDETERMINED?

WHY IS IT SOMETIMES DIFFICULT OR IMPOSSIBLE TO COME TO A DETERMINATION?

In almost all cases the cause of death is determined, but manner of death is more complicated. Cause of death is determining what physiological, anatomic problem caused the death of the victim. Manner of death is determining how the death occurred. For example, a gunshot victim’s cause of death is a gunshot wound. That victim’s manner of death would then have to be determined as homicide, suicide or accident. Determining manner of death is based on more factors than just the autopsy and will include investigative information and the police report. The State’s Attorney and law enforcement will make determinations that may be different from ours. For example, we may call a homicide may be determined to be a justifiable homicide by the State’s Attorney’s Office and therefore no one is charged. Or, we consider an accident may be ruled otherwise by the police or the State’s Attorney’s Office.

WHAT IS A TYPICAL WEEK LIKE IN YOUR OFFICE? I.E. HOW MANY AUTOPSIES ARE PERFORMED, HOW MANY SCENE/SITE VISITS ARE MADE, WHAT OTHER TYPE OF WORK IS PERFORMED IN OR BY THE OFFICE?

An average week will include 100 autopsies, 200 scene visits and toxicology on 120 cases.

WHEN IS THE MEDICAL EXAMINER REQUIRED TO MAKE THE DETERMINATION OF DEATH AND WHEN CAN IT BE MADE BY A DOCTOR OR OTHER MEDICAL PRACTITIONER?

Any non-natural death must be reported to the Office of the Chief Medical Examiner. If a doctor is willing to sign a death certificate at the scene, the victim will be transported to a funeral home and we will not become involved. In a situation where there is no doctor willing or able to sign a death certificate on scene, or there are suspicious or violent circumstances, the Medical Examiner must be called to the scene.

WHEN IS AN AUTOPSY REQUIRED?

This is determined by the Medical Examiner investigator at the scene who will interview witnesses, family members, speak to the police, review medical history and take any other circumstances into account. The investigator works with a Medical Examiner by phone to make the determination as to whether the body should be transported for an autopsy or the body will be transported to a funeral home and a death certificate can be signed by the Medical Examiner’s Office without an autopsy.

HOW OFTEN IS THE CAUSE OF DEATH UNDETERMINED?

WHY IS IT SOMETIMES DIFFICULT OR IMPOSSIBLE TO COME TO A DETERMINATION?

In almost all cases the cause of death is determined, but manner of death is more complicated. Cause of death is determining what physiological, anatomic problem caused the death of the victim. Manner of death is determining how the death occurred. For example, a gunshot victim’s cause of death is a gunshot wound. That victim’s manner of death would then have to be determined as homicide, suicide or accident. Determining manner of death is based on more factors than just the autopsy and will include investigative information and the police report. The State’s Attorney and law enforcement will make determinations that may be different from ours. For example, we may call a homicide may be determined to be a justifiable homicide by the State’s Attorney’s Office and therefore no one is charged. Or, we consider an accident may be ruled otherwise by the police or the State’s Attorney’s Office.

WHAT IS A TYPICAL WEEK LIKE IN YOUR OFFICE? I.E. HOW MANY AUTOPSIES ARE PERFORMED, HOW MANY SCENE/SITE VISITS ARE MADE, WHAT OTHER TYPE OF WORK IS PERFORMED IN OR BY THE OFFICE?

An average week will include 100 autopsies, 200 scene visits and toxicology on 120 cases.
DO MEDICAL EXAMINERS AND INVESTIGATORS RECEIVE ANY PSYCHOLOGICAL TRAINING TO HELP DEAL WITH THE EMOTIONAL IMPACT OF THEIR WORK?

This type of work really self-selects people who are able to manage the psychological aspect of performing autopsies. By the time they are working in the Medical Examiner’s office, they have been through medical school, pathology, autopsies and forensic training. Since Medical Examiners do not typically respond to scenes, they are used to working with bodies in a clean, quiet, sterile, climate controlled area, which does not present the type of emotional or psychological impact that working at a scene might present. Therefore, this is more of a concern for forensic investigators who must deal with the trauma and stress at a scene.

DAVID FOWLER, native of Rhodesia—now known as Zimbabwe—David R. Fowler attended medical school at University of Cape Town in South Africa and completed a five-year residency in forensic pathology. Dr. Fowler came to the U.S. in 1991 for a residency in anatomic pathology at University of Maryland Medical Center. He did a two-year fellowship in forensic pathology at the Office of the Chief Medical Examiner and remained as an Assistant Medical Examiner. Dr. Fowler was promoted to Deputy Chief Medical Examiner in 1998 and named Chief Medical Examiner in 2002.

Dr. Fowler has had numerous articles published in medical journals, and his work has been included in a number of books. He holds numerous professional memberships and committee positions and teachingships and committee positions and teaching services and lectures to federal, state and local agencies and organizations. Established in 1939 as the country’s first statewide medical examiner’s office, OCME today is the largest freestanding forensic medical centers in the U.S.

CAROLYN HESS JOHNSON, ESQ., is an attorney and a full-time Professor of Forensic Studies in the School of Graduate and Professional Studies at Stevenson University. She has worked in private practice, as a Senior Assistant State Prosecutor for the State of Maryland and as an Assistant State’s Attorney in Baltimore City, Maryland.

Carolyn Hess Johnson

Interview conducted on Friday, December 14, 2012:

JUDGE BATTAGLIA, YOU HAVE WRITTEN THE COURT’S TWO LEADING DECISIONS ON THE ADMISSIBILITY OF SCIENTIFIC OPINION EVIDENCE IN THE CLEMMONS AND BLACKWELL CASES. COULD YOU EXPLAIN THEIR SIGNIFICANCE?

Both cases explore the interaction of science and law. In Blackwell v. West, the issue was the relationship of thimerosal, a preservative found in childhood vaccines, and autism in children. The premise was that some children, but not all, who received vaccines with thimerosal developed autism. A scientist developed the theory that thimerosal caused autism in children, but then he qualified his theory to thimerosal triggering a genetic predisposition to autism in children. The trial judge, Stuart Berger of the Circuit Court for Baltimore City (now on the Court of Special Appeals) conducted a week long hearing in which he examined the qualifications of the experts to testify regarding the relationship of thimerosal to autism, and whether there was any causal connection between the two.

Judge Berger believed that his role as a trial judge was to be the gatekeeper in deciding the admissibility of the evidence. He determined that the premise that thimerosal was related to autism was not sound, the theory did not meet the standard of reliability found in “Frye/ Reed” and there was no scientific causal connection between the drug and autism. When the Court of Appeals looked at the case, we not only examined his legal conclusions de novo but agreed with his finding that the offered “science” did not meet the standards of “Frye/ Reed”, derived from a decision of the Court of Appeals in 1978 in Reed v. State. In writing the Blackwell decision, I was able to explore the interaction of science and law and realized that scientific standards are much more rigorous than law because we have no test tube in law nor do we have the ability to replicate the human experience.

Scientists are skilled at withholding critical analysis, whereas lawyers are required to develop critical analysis and apply it instantaneously. In science, the ability to replicate the method and results is the cornerstone of reliability. We can never replicate human experience in law. So the search for truth in science is really very different than in law.

In Blackwell the Court recognized the gate-keeping role of the trial judge when it comes to scientific evidence, a position not without controversy among some judges who believe it should be up to the jury to decide the validity of the science. We felt it was important to maintain confidence in the court system to keep bad science out.

Clemmons presented the unusual situation of what to do when reliability and validity of a scientific theory have eroded. We looked at the science behind Comparative Bullet Lead Analysis (CBLA) that had been widely accepted and found that the theory upon which it was based was no longer sound today. Its acceptance had eroded over time and scientists in the field did not believe it to be reliable nor valid today.

Both DECISIONS SEEM TO REFLECT THE RECOGNITION OF THE POWER OF SCIENTIFIC EVIDENCE, WOULD YOU AGREE?

Yes, junk science, science based on false premises or an analytical gap (the use of sound data in an unsound way) can drive verdicts and produce unjust results. It may adversely affect people’s faith in the judicial system by producing unjust results.

WHAT CAN OUR STUDENTS WHO ARE BEING TRAINED IN HOW TO BECOME EXPERT WITNESSES TAKE FROM THESE CASES? ARE THERE LIMITS ON TESTIMONY?

It depends on the role. Whether the student is going to be testifying as an expert or investigator. If testifying as experts, students must become familiar with the state of the law and the state of the science. They must be prepared to address the changes that may have occurred in the science or its reputation. If engaged in litigating, experts must be prepared to present arguments for or against the science. At the same time, experts must take care not to become advocates. Once the expert becomes an advocate, he/she loses all credibility.

With established science, if problems occur, it is usually because the expert has overstated the premise. Instead of finding a connection or correlation, it becomes 100% that X proves Y, when no scientist would ever say that. Science is never 100% anything. When an expert looks at a theory as an absolute or becomes invested in results, problems will ensue.

One of the major correlations between law and science is that both involve due process. In law, it is generally shorter, resolution oriented and involves due process. With science, there is a similar process but over a longer period of time. Experts who are results oriented are really short circuiting the process.

AS A JUDGE PRESIDING OVER CASES INVOLVING THE INTERRELATION OF SCIENCE AND LAW, HOW DOES ONE PREPARE?

In the shift to a different role from prosecutor to judge, I have learned just how much I don’t know, a humbling experience, but a process that allows me to divorce myself from results. It has been one of the best things that has happened to me in this job. I have been able to explore the vastness of knowledge. To write Blackwell was a gift to me.
DO JUDGES HAVE TO BECOME SUBJECT MATTER EXPERTS? ARE THERE FORMAL TRAINING PROGRAMS FOR MARYLAND JUDGES?

Judge Robert Bell, our Chief Judge and one of the founders of ASTAR (Advanced Science and Technology Adjudication Resource Project) nationally, has made a significant investment in the training and education of our judges. This will be his legacy when he retires later this year.

With federal funding, Judge Bell initiated the ASTAR program for trial and appellate judges to train them in various aspects of science in order to understand the scientific method. We have covered genetics, DNA, brain scans, and addiction, not to be subject matter experts, but to understand the analytical process and learn the scientific method. I can't think of an area of science that we have not discussed behind the trend. We only get the case after it makes its way through the Court of Appeals feels is important.

WHO ARE YOUR PARTNERS IN ASTAR?

We are fortunately situated in the midst of some of the most important scientific research institutions in the country, so we have partnered with the National Institute of Mental Health, National Institute of Health, and Johns Hopkins. We have judges coming from all over the country to attend our programs.

DO YOU SEE ANY TRENDS IN THE ACCEPTANCE AND HANDLING OF EXPERT WITNESSES?

The Court does not select its cases and so it follows somewhat slowly is just some resistance to the regulation but we all agree that no lawyer can stay stagnant and still be successful.

DO YOU SEE ANY TRENDS IN THE ACCEPTANCE AND HANDLING OF EXPERT WITNESSES?

When I came on the bench in 2001, the Maryland State Bar Association had recommended similar training for experienced lawyers. The concern was that some lawyers and judges did not have a real sense of professionalism. We, on the Court, felt that we needed an understanding of the status of professionalism throughout the state.

I led the Task Force on Professionalism and with Chief Judge Bell and others visited every county in Maryland and conducted open hearings with members of the Bar in attendance to explore: what was the sense of professionalism in that locale, was it waning or waning, the reasons why and if waning, the ways to deal with it. In most every county, there was a general sense that professionalism, defined in different ways in terms of civility and ethics, was declining. A large part of the problem involved practice areas such as domestic law, motivated by clients' desire for "Rambo style" lawyering or it was facilitated by advances in the use of technology allowing for fast, sometimes unguarded communication.

An outcome of that work, we just announced the opening of the Center for Professionalism, a quasi-judicial agency which will be responsible for conducting the training for the newly admitted lawyers in a day-long program as well as a mentoring program.

The next wave will be dealing with aging attorneys, multi-jurisdictional cases, substance abuse in attorneys, and mandatory CLE for all lawyers.

WE RECOGNIZE THE NEED FOR A PROFESSIONALISM COURSE FOR EXPERIENCED LAWYERS.

Your students are entering their professions at a wonderful time for most current developments in their field, the better they will be as witnesses. It is important to have the credentials and education but still will not be successful without the ability to communicate. Your students are entering their professions at a wonderful time for the exploration of the technology and science. They must be prepared as they are entering a brave new world. They are going to have the opportunity to explore advances that we cannot even anticipate, but they must have the ability to communicate their experience. I wish them the best as they navigate and lead.

If I had my druthers, there would be mandatory mentoring by experienced attorneys for all newly admitted lawyers. The mentoring aspect of the Center is based on the recognition that we are a community that functions well based on relationships with each other. Relationship skills are not taught in law school. I see mentoring as a vehicle to show young lawyers how to become integrated in the society of lawyers.

WHAT ADVICE DO YOU HAVE FOR THE STUDENTS IN OUR PROGRAMS WHO FIND THEMSELVES INVOLVED AS WITNESSES IN LITIGATION?

The biggest thing is to be prepared. That seems so hackneyed but it is not. More the students understand and are able to communicate the basis of the opinion, as well as be so thoroughly familiar with the most current developments in their field, the better they will be as witnesses. It is important to have the credentials and education but still will not be successful without the ability to communicate. Your students are entering their professions at a wonderful time for the exploration of the technology and science. They must be prepared as they are entering a brave new world. They are going to have the opportunity to explore advances that we cannot even anticipate, but they must have the ability to communicate their experience. I wish them the best as they navigate and lead.
Approaches to Library Research in Forensics
Maureen Beck and Sara Godbee

The twenty-first century researcher now has a wealth of tools at her or his fingertips to help overcome information overload and achieve targeted search results. The latest discovery tools and new reference management software enable the researcher to achieve a high level of organization and precision in conducting research. This article will suggest a few ways to approach library research in the area of forensic studies, including recommended strategies and specific resources.

Obviously, the researcher must cover multiple disciplines for this very complex field, possibly tapping into research in criminology, sociology, computer science, psychology, law, medicine, etc., depending on the nature of the specific topic. One traditional approach is to choose databases with coverage in the relevant disciplinary areas, searching each database separately. It is also possible with some vendors like EBSCOhost to select multiple databases and search them simultaneously. However, there is almost always a loss in precision because of the differences in the ways individual databases are organized, even ones from a single vendor. Furthermore, each database has its own discipline-specific vocabulary and it is crucial to learn how to work with this feature to maximize search results. It can be helpful to browse through the thesaurus of terms for each database and keep a running list of search terms as the researcher works through the process. Another helpful technique is to locate one or two good articles and incorporate the subject terms assigned to the article into a new search statement. In addition, the researcher can scan the article summary or abstract for different helpful keywords.

One of the latest developments for researchers is the so-called discovery tool, now offered by many academic libraries. Stevenson University calls its discovery service One Search, because it searches across hundreds of databases simultaneously and eliminates the need to select a single database based on coverage of a discipline relevant to the topic. An embedded knowledge-base helps One Search to achieve highly relevant search results. One Search also covers the library’s online catalog. Thus, a search result will include citations to books, both print and electronic, journals, magazines, newspapers, government documents and other reports, and other categories of credible publications. The process begins at the Stevenson University Library webpage (http://stevensonlib.org). The researcher will first enter the keywords in the search box prominently situated in the middle of the screen. Once the results screen appears, the viewer will see, on the left side, facets, or options for focusing or narrowing the search by subject, date, type of resource, or content provider, among others.

Another challenge to today’s researcher can be organizing and keeping track of all the information they gather while researching. Fortunately, databases and discovery tools include options for creating research folders to store retrieved documents along with emailing options. In addition, the modern researcher can use online reference management tools developed to help the researcher organize, store and retrieve the sources they have gathered in their research efforts.

Reference management tools like Zotero and Connotea capture bibliographic information for online sources from websites to library catalogs and databases. These and similar tools are free or offer free versions and are either web-based or can be synthesized from one computer or device to another. Through each reference management tool works in its own unique way, they all offer similar features to the serious researcher making it easy to organize and track research sources.

Zotero, originally designed as a Mozilla Firefox extension, now offers a stand-alone or computer-based version with connectors for Google Chrome and Safari web browsers. Zotero allows users to capture information about all types of items with records accessible on the web. From a book in a catalog to a sound recording online, Zotero will capture bibliographic information about an item along with web addresses and file attachments when available.

Zotero allows for organization of reference sources within collections along with tagging, thus making locating stored items easier. In addition, Zotero can produce bibliographic entries for the items stored in a collection. With the use of word processor plug-ins, a complete bibliography of sources used in a research project can be exported from the Zotero stored information. (www.zotero.org)

Connotea is an online or web-based reference management tool targeted to the academic and scientific researcher. It allows users to gather resources found online by saving the link to the web page where the source was located. Connotea then adds the bibliographic information. Because this tool is web-based, the user is computer independent and can add documents or web pages to their resource collection wherever and whenever they find it without the need to synch their account.

Connotea allows users to import and export libraries of resources from computer-based reference management tools. It also has a strong focus on sharing found information with other users interested in the same area of study by allowing users to view collections built by other users. (www.connotea.org)

With this plethora of new approaches, research in forensic studies can become more manageable for the forensic studies scholar.

MAUREEN BECK has a B.A. in English and Anthropology from Indiana University of Pennsylvania, the Master’s degree and the Advanced Certificate in Library Science from the University of Pittsburgh, and the Master’s degree in Administrative Science from the John Hopkins University. She has worked at large research institutions including the University of Pittsburgh Library System and the E. I. du Pont de Nemours and Company (now the Sheridan Libraries) at the John Hopkins University. She has been Director of Library Services at Stevenson University since January of 2000.

SARA GODBEE, MLS Sara received her MLS from the University of Maryland College Park in December, 2007. While completing her MLS, Sara served as the Library Associate at the University of Maryland College managing the day-to-day operations of Document Management’s Interlibrary Loan services and a team of library assistants.

Sara joined Stevenson University in September, 2008 as the first librarian for the School of Business and Leadership. In this role, she manages the university’s business, law and information technology collections. She also serves as the liaison librarian to all the departments within the School of Business and Leadership, as well as, the graduate programs for Business & Technology Management and Forensic Studies.
The United States (U.S.) faces a significant threat to its currency: the counterfeiting of U.S. currency. The sophisticated technology used in counterfeit bills is nothing new, Supernote counterfeits are not ordinary counterfeits. They are printed on the same high-quality, cotton-linen blend that the U.S. government uses. The printing also engraves the bills and utilizes special, color-shifting ink that is generally only sold to government agencies. Dr. Stephen Mihm, in his New York Times article, “No Ordinary Counterfeit,” identifies many of the security features that accurately reproduce. Dr. Mihm, in his New York Times article, identifies many of the security features that the Supernote counterfeiter utilizes. In 1990, North Korea purchased several high-speed, intaglio presses – the same kind that could be used to produce bank notes – for approximately $19 million (Rose, 4). The use of forensic financial investigations to support actions, such as asset forfeiture in criminal cases or the use of financial sanctions, is an effective method to help neutralize the money-laundering component of this crime. The counterfeiter must engage in financial transactions to effectively trade counterfeit currency for items of value. Disrupting the financial aspects of the scheme reduces their ability to profit from counterfeiting and leads to a reduction in the criminal activity.

UNDERSTANDING SUPERNOTES

What differentiates a Supernote from a typical counterfeit bill? U.S. paper money contains numerous features that make it difficult to accurately reproduce. Dr. Stephen Mihm, in his New York Times article, “No Ordinary Counterfeit,” identifies many of the security features of U.S. currency emanating from the 1996 redesign. The paper utilized for U.S. currency is an expensive blend of cotton and linen fibers in a ratio of about 5:1. The ink in the printing is known as Optically Variable Ink (OVI) which shifts color depending on the light and how the bill is held. Bills also contain micro-printing, a watermark, a metallic security thread, and the distinctive head portrait. Even the printing method used is a security feature. The U.S. uses intaglio printing to manufacture its currency, which utilizes high-pressure engraving plans to strike the bill with ink, creating its unique look and feel (Engber).

U.S. law enforcement divides counterfeiting into three categories: off-the-shelf lithography, digital production, and Supernotes (Engber). Although off-the-shelf and digital technology can produce quality reproductions, they cannot replicate the look and feel of U.S. currency. To accomplish this, the security features must be replicated almost flawlessly; while using the same materials – paper, ink, and intaglio printing (Engber; the President’s Commission on the U.S. Government). This is a small task and not likely to be accomplished by petty criminals. It clearly speaks to a well-orchestrated, well-financed operation that can facilitate a large-scale criminal enterprise. Many believe this is only possible through state-sponsored activity. According to Steven Mihm, “in theory, only governments can buy intaglio printing presses used for making money, and only a handful of companies sell them” (Mihm). So who is behind the production of Supernote? According to many U.S. government officials, North Korea. According to many U.S. government officials, North Korea is involved in the production and distribution of counterfeit U.S. Supernotes.

“EVIDENCE OF NORTH KOREAN COUNTERFEITING

“The North Koreans have denied that they are engaged in the distribution and manufacture of counterfeit currency, but the evidence is overwhelming that they are. There’s no question of North Korea’s involvement” stated Daniel Glaser, Deputy Assistant Treasury Secretary for Terrorism Financing and Financial Crimes (Mihm). Glaser’s statement is bolstered by anecdotal evidence supporting North Korea’s capabilities. In 1990, North Korea purchased several high-speed, intaglio presses – the same kind that could be used to produce bank notes – for approximately $19 million (Rose, 4). The use of forensic financial investigations to support actions, such as asset forfeiture in criminal cases or the use of financial sanctions, is an effective method to help neutralize the money-laundering component of this crime. The counterfeiter must engage in financial transactions to effectively trade counterfeit currency for items of value. Disrupting the financial aspects of the scheme reduces their ability to profit from counterfeiting and leads to a reduction in the criminal activity.

THE ENTERPRISE CONTINUES

There is hard evidence of direct North Korean involvement with the production of counterfeit U.S. currency. In 1998, law enforcement authorities arrested three North Korean trading company executives, traveling with Diplomatic passports, for attempting to deposit over $250,000 in Supernote in a Macau bank (Tkacik). The Japanese Navy seized a North Korean spy-ship in its territorial waters in 1998, discovering millions in counterfeit U.S. Supernote abroad (Tkacik). A 2007 Congressional Research Service report detailing North Korean criminal activities cites thirteen known incidents of North Korean enterprises – embassy personnel, diplomats, officials of state-owned companies, and others – directly involved in producing and/or passing counterfeit U.S. currency. These thirteen incidents occurred in Asia and Europe (Perl and Nanto, North Korean Counterfeiting). More recently, U.S. law enforcement authorities have initiated prosecutions of individuals connected to North Korea for their involvement in Supernote counterfeiting. In 2005, two U.S. law enforcement operations, dubbed Royal Charm and Smoking Dragon, culminated in dozens of indictments and included the seizure of approximately $4 million in counterfeit Supernote Supernote being smuggled into the United States. After the arrests, the President’s Commission on the U.S. Government classified North Korea as “a major criminal organization involved in the production of counterfeit currency. The enterprise continues because the economic infrastructure remains intact...” According to the Financial Investigations Guide published by the Asset Forfeiture and Money Laundering Section (AFMLS) of the U.S. Department of Justice, the “enterprises, including the production of Supernotes (Asher, 2011, 39). Surprisingly, however, several large scale investigations were never fully realized or were halted altogether (Asher, 2011, 45). The focus of forensic financial investigations into North Korean production of Supernote will be explored in the following examples.

FINANCIAL FORENSIC INVESTIGATIONS

There are numerous publications detailing North Korea’s criminal enterprises, including the production of Supernote. Most address the “what” aspects of these crimes – counterfeiting currency, illegal drug production and distribution, manufacturing of counterfeit prescription drugs and cigarettes – but fail to discuss the “how” of the financial transactions necessary to profit from these crimes. Counterfeiting money has no value until it is spent. The typical petty counterfeiter can pass a few counterfeit bills at a retail store to obtain goods or purchase a small dollar item with a higher denomination fake, thereby exchanging the counterfeit for genuine change. Obviously, a national government cannot go to a shopping mall and spend $25 million in counterfeit bills. For North Korea to successfully integrate Supernotes on large scale, transactions involving financial institutions, businesses, and individuals must occur. These transactions could become very simple – the exchange of counterfeit bills for goods. However, that approach becomes unwieldy as the amounts increase. Large cash transactions raise questions as they are bulky, risky, and attract the wrong kind of attention – from banking authorities, regulators, and law enforcement agencies. A far better plan is to enlist sophisticated criminal organizations, including state-sponsored ones, to integrate the financial system, to involve money laundering, thus easing the flow of proceeds towards prosecution. The charges filed could include asset forfeiture counts to seize ill-gotten gains from bank accounts or property purchased by manipulating counterfeit currency. If the scheme involved a regulated industry, such as investments or insurance, regulatory code could be used to file cease and desist actions against the entity. Block the proceeds flowing to that industry again, and/or take the business into government receivership. The use of financial forensic investigations to identify criminal or regulatory violations is a powerful weapon against crime. According to the “Financial Investigations Guide” published by the Asset Forfeiture and Money Laundering Section (AFMLS) of the U.S. Department of Justice, “the enterpris...” Financial investigations deal with the financial components involved in these crimes and identify what violations might be prosecutable. As an example, a law enforcement agent conducting a money-laundering investigation has to understand both the mechanisms of the transactions in question and how each transaction satisfies the elements of statutory criminal violations. Once discovered, such violations could be used to take action against the perpetrators. Using the money-laundering example, once evidence is discovered that federal laws were violated, the agent proceeds towards prosecution. The charges filed could include asset forfeiture counts to seize ill-gotten gains from bank accounts or property purchased by manipulating counterfeit currency. If the scheme involved a regulated industry, such as investments or insurance, regulatory code could be used to file cease and desist actions against the entity. Block the proceeds flowing to that industry again, and/or take the business into government receivership. The use of financial forensic investigations to identify criminal or regulatory violations is a powerful weapon against crime. According to the “Financial Investigations Guide” published by the Asset Forfeiture and Money Laundering Section (AFMLS) of the U.S. Department of Justice, “the enterpris...” Financial investigations deal with the financial components involved in these crimes and identify what violations might be prosecutable. As an example, a law enforcement agent conducting a money-laundering investigation has to understand both the mechanisms of the transactions in question and how each transaction satisfies the elements of statutory criminal violations. Once discovered, such violations could be used to take action against the perpetrators. Using the money-laundering example, once evidence is discovered that federal laws were violated, the agent proceeds towards prosecution. The charges filed could include asset forfeiture counts to seize ill-gotten gains from bank accounts or property purchased by manipulating counterfeit currency. If the scheme involved a regulated industry, such as investments or insurance, regulatory code could be used to file cease and desist actions against the entity. Block the proceeds flowing to that industry again, and/or take the business into government receivership. The use of financial forensic investigations to identify criminal or regulatory violations is a powerful weapon against crime. According to the “Financial Investigations Guide” published by the Asset Forfeiture and Money Laundering Section (AFMLS) of the U.S. Department of Justice, “the enterpris...” Financial investigations deal with the financial components involved in these crimes and identify what violations might be prosecutable. As an example, a law enforcement agent conducting a money-laundering investigation has to understand both the mechanisms of the transactions in question and how each transaction satisfies the elements of statutory criminal violations. Once discovered, such violations could be used to take action against the perpetrators. Using the money-laundering example, once evidence is discovered that federal laws were violated, the agent proceeds towards prosecution. The charges filed could include asset forfeiture counts to seize ill-gotten gains from bank accounts or property purchased by manipulating counterfeit currency. If the scheme involved a regulated industry, such as investments or insurance, regulatory code could be used to file cease and desist actions against the entity. Block the proceeds flowing to that industry again, and/or take the business into government receivership. The use of financial forensic investigations to identify criminal or regulatory violations is a powerful weapon against crime. According to the “Financial Investigations Guide” published by the Asset Forfeiture and Money Laundering Section (AFMLS) of the U.S. Department of Justice, “the enterpris...” Financial investigations deal with the financial components involved in these crimes and identify what violations might be prosecutable. As an example, a law enforcement agent conducting a money-laundering investigation has to understand both the mechanisms of the transactions in question and how each transaction satisfies the elements of statutory criminal violations. Once discovered, such violations could be used to take action against the perpetrators. Using the money-laundering example, once evidence is discovered that federal laws were violated, the agent proceeds towards prosecution. The charges filed could include asset forfeiture counts to seize ill-gotten gains from bank accounts or property purchased by manipulating counterfeit currency. If the scheme involved a regulated industry, such as investments or insurance, regulatory code could be used to file cease and desist actions against the entity. Block the proceeds flowing to that industry again, and/or take the business into government receivership. The use of financial forensic investigations to identify criminal or regulatory violations is a powerful weapon against crime. According to the “Financial Investigations Guide” published by the Asset Forfeiture and Money Laundering Section (AFMLS) of the U.S. Department of Justice, “the enterpris...” Financial investigations deal with the financial components involved in these crimes and identify what violations might be prosecutable. As an example, a law enforcement agent conducting a money-laundering investigation has to understand both the mechanisms of the transactions in question and how each transaction satisfies the elements of statutory criminal violations. Once discovered, such violations could be used to take action against the perpetrators. Using the money-laundering example, once evidence is discovered that federal laws were violated, the agent proceeds towards prosecution. The charges filed could include asset forfeiture counts to seize ill-gotten gains from bank accounts or property purchased by manipulating counterfeit currency. If the scheme involved a regulated industry, such as investments or insurance, regulatory code could be used to file cease and desist actions against the entity. Block the proceeds flowing to that industry again, and/or take the business into government receivership. The use of financial forensic investigations to identify criminal or regulatory violations is a powerful weapon against crime. According to the “Financial Investigations Guide” published by the Asset Forfeiture and Money Laundering Section (AFMLS) of the U.S. Department of Justice, “the enter...
the BSA was originally passed in 1970 in an effort to curtail forfeiture (U.S., Asset Forfeiture, Appendix A-1). Under the concept of asset forfeiture, the U.S. can seek to seize in counterfeit U.S. currency (U.S., DOJ, Asset Forfeiture, Appendix A-1). The U.S. can assert criminal jurisdiction over international counterfeiting of U.S. issued obligations and prosecute these crimes within the criminal justice system. The U.S. must also utilize other means, such as Treaties dealing with the extradition of criminals charged in the U.S. to facilitate prosecution. The United States has extradition treaties with scores of countries to facilitate the arrest and extradition of international criminals (“Extradition Treaties”).

The use of asset forfeiture violations charged contemporaneously with other crimes is a powerful tool against criminal activity. The U.S. has codified numerous Mutual Legal Assistance Treaties (MLATs) with many countries (”Treaties and Agreements”). According to the Department of State, “Mutual Legal Assistance Treaties (MLATs) allow generally for the exchange of evidence and information in criminal and ancillary matters. In money laundering cases, they can be extremely useful as a means of obtaining banking and other financial records from our treaty partners (“Treaties and Agreements”).”

Through MLATs, the United States can obtain evidence of crimes that have occurred internationally. This evidence can be admitted in U.S. courts for criminal prosecution. It behooves these foreign governments to cooperate as well; the U.S. Department of Justice has shared over $229 million in forfeited assets with cooperating states (“Treaties and Agreements”). The use of forensic financial investigations through MLATs has a powerful financial impact on criminal organizations. The U.S. also uses Executive Agreements and Letters of Rogatory to obtain international cooperation in criminal investigations (U.S. Internal Revenue Manual, 9.7.10). Executive Agreements typically support existing MLATs while a Letter Rogatory would be a formal request from the United States to a foreign power for assistance (U.S. Internal Revenue Manual, 9.7.10.2.3, 9.7.10.2.4).

Section 311 of the PATRIOT Act and the use of sanctions are very powerful tools utilized by U.S. law enforcement and regulatory entities to combat international criminal activity. The USA PATRIOT Act was signed into law on October 26, 2001 in the wake of the September 11th terrorist attacks against the U.S. (U.S., Federal Register, 12730 - 12731). This law strengthened the existing Bank Secrecy Act and empowered the Director of FinCEN with, “the authority, after finding that reasonable grounds exist for concluding that a foreign jurisdiction, institution, class of transactions, or type of account is of primary money laundering concern” (U.S., Federal Register, 12731). Once an entity is labeled as a money laundering concern under Section 311, the U.S. can seek to levy a charge of money laundering, which has both criminal and civil asset forfeiture provisions (U.S., DOJ, Asset Forfeiture, Appendix A-3). Under this law, the U.S. can seek to seize proceeds of criminal activity or property utilized to facilitate crimes. Additionally, the U.S. has criminalized money laundering in 18 USC 1956 and 18 USC 1957 (“USC Title 18”). A Suspicious Unlawful Activity (SUA), as defined by statute, must have occurred to substantiate the crime of money laundering (U.S., DOJ, Asset Forfeiture, Appendix A-3). Thus, the crimes involved in counterfeiting U.S. currency internationally can be charged in the U.S., and any profits or property that can be linked by the financial investigation could be subject to forfeiture (U.S., Asset Forfeiture, Appendix A-3).

Another powerful financial investigative tool is the Bank Secrecy Act (BSA). The BSA was originally passed in 1970 in an effort to curtail money laundering (“Bank Secrecy Act”). The U.S. Criminal Financial Enforcement Networks (FinCEN) web page outlining the BSA identifies a number of its requirements. “… the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities.” (“Bank Secrecy Act”). Financial institutions (and certain other entities such as casinos) must file reports with FinCEN under the BSA; these include Currency Transaction Reports (CTRs), which identify cash transactions over $10,000, and Suspicous Activity Reports (SARs), which are used to report suspicions of money laundering or other criminal activity (U.S., Internal Revenue Manual, 9.5.1.yw). These filings are available to U.S. government agencies to assist with law enforcement investigations into money laundering (“Bank Secrecy Act”).

The U.S. law enforcement has an international aspect as well. The U.S. has signed numerous Mutual Legal Assistance Treaties (MLATs) with many countries (“Treaties and Agreements”). According to the Department of State, “Mutual Legal Assistance Treaties (MLATs) allow generally for the exchange of evidence and information in criminal and ancillary matters. In money laundering cases, they can be extremely useful as a means of obtaining banking and other financial records from our treaty partners (“Treaties and Agreements”).”

In Section 311 of the PATRIOT Act, the use of sanctions are very powerful tools utilized by U.S. law enforcement and regulatory entities to combat international criminal activity. The USA PATRIOT Act was signed into law on October 26, 2001 in the wake of the September 11th terrorist attacks against the U.S. (U.S., Federal Register, 12730 - 12731). This law strengthened the existing Bank Secrecy Act and empowered the Director of FinCEN with, “the authority, after finding that reasonable grounds exist for concluding that a foreign jurisdiction, institution, class of transactions, or type of account is of primary money laundering concern” (U.S., Federal Register, 12731). Once an entity is labeled as a money laundering concern under Section 311, the U.S. can take action to curtail the entity’s activities. Per a Treasury Department Fact Sheet:

The following special measures can be imposed individually, jointly, in any combination and in any sequence:

• Record keeping and reporting certain transactions;
• Collection of information relating to beneficial ownership;
• Collection of information relating to certain payable-through accounts;
• Collection of information relating to certain correspondent accounts;
• Prohibition or conditions on the opening of or maintaining of correspond- ent or payable-through accounts. (“Fact Sheet”) The U.S. can, in effect, compel information on who is behind transactions, gather information on the transactions in question, and limit the ability of an entity to do business in the U.S. financial system. The last point is significant: the U.S. can literally freeze entities out of its financial system. This is extremely powerful in that it can cripple businesses. How many international financial institutions could service their customers if they were frozen out of doing business with U.S. financial institutions? This particular tool was extremely effective against North Korea.

The Treasury Department’s Office of Foreign Asset Control (OFAC) utilizes sanctions to control criminal or aggressive foreign entities (“About”). These sanctions are economic in nature and can prohibit trade, travel, or other interactions with foreign entities. The U.S. has utilized sanctions against North Korea for years (“About”). Currently, the U.S. has blocked many financial and property transactions with North Korean entities (“OFAC Sanctions Matrix”).

The United States is also a participant in the Financial Action Task Force (FATF). FATF is an organization of over 30 countries that sets standards and policies aimed at reducing money laundering and other crimes, such as terrorist financing (“An Introduction to FATF”). Through FATF participation, countries self-regulate money laundering laws and standards. They also pledge mutual cooperation, such exchanging information between financial agencies (“An Introduction to FATF”). FATF’s recommendations are, “the internationally endorsed global standards for implementing effective AML/CFT measures. They increase the transparency of the financial system (making it easier to detect criminal activity) and give countries the capacity to successfully take action against money launderers and terrorist financiers” (“An Introduction to FATF”). Many FATF recommendations are incorporated into treaties and United Nations Resolutions (“An Introduction to FATF”).

CASE EXAMPLES: FINANCIAL FORENSIC INVESTIGATIONS INVOLVING NORTH KOREAN COUNTERFEITING

Many of the tools discussed above have been successfully utilized in investigations of North Korean counterfeiting of Supernotes, leading to a number of high-profile arrests, seizures, and sanctions. These cases all utilized financial forensic investigations in some capacity. The following examples will explore the successes and shortcomings of these techniques with respect to Supreme counterfeiting.

The best known cases that introduced the world to Supernotes were two inter-related investigations, code named Royal Charm and Smoking Dragon (Mihm). These investigations were initiated by the F.B.I. and consisted of numerous federal and state law enforcement agencies. Both investigations connected similar activities, groups, and individuals related smuggling operations (“About”). Operation Royal Charm began in New Jersey and involved smuggling contraband through the Port of Newark, while Operation Smoking Dragon occurred in the Port of Los Angeles (“About”). Both investigations dealt with extreme criminal activity: smuggling counterfeit cigarettes, illegal drugs and weapons, and counterfeits Supernotes (“Operation Smoking Dragon”). The counterfeit currency was smuggled into the United States via secret compartments in shipping containers aboard vessels which had falsely listed their port of origin as being from China versus North Korea; these Supernotes were originally purchased for less than 40 cents on the dollar (U.S., Statement of David Adker). Once in the United States, the contraband could be distributed through criminal networks for sale or for the counterfeit notes introduced into the U.S. financial system. One means of laundering the notes into the financial system was through casinos in Las Vegas, which was perpetrated to a significant degree by Chen Ching Luei (Rose, 3). The scheme worked as follows: Liu was a main player identified in Operation Smoking Dragon, dealing directly with undercover law enforcement agents as they investigated the smuggling operation. He routinely traveled from his home in California to Las Vegas to smuggle counterfeit notes into the casinos. Liu would spend thousands in counterfeit notes in slot machines, but only place small bets. He would then redeem the unspent balance, thus exchanging counterfeit notes for real money (“About”). Between 2005 and 2007, investigation by law enforcement determined that he spent over $5.5 million dollars in this manner, although it is unknown what percentage of this were Supernotes bills (Rose, 3). In an unrelated case, Mei Ling Chen was arrested by federal authorities after she was implicated in smuggling Supernotes into the U.S. (Rose, 3). Chen’s scheme involved spending the Supernotes on luxury goods, then returning them for refunds. Thus, Supernotes were exchanged for real currency through a financial transaction (Rose, 4)
The above cases illustrate the financial transaction aspects of the cornerstone of Supreme’s use of the U.S. financial system. In each case, the counterfeit bills were integrated via a monetary transaction to effectively exchange Supernotes for real currency. This highlights why forensic financial investigations are important; once the counterfeit notes are detected, the transaction can be traced backwards to iden-
tify the source. In Chen’s case, Secret Service agents were tipped to the Supreme smuggling via a U.S. Customs search of an incoming package (Rose, 4). Once she was arrested, the Secret Service con-
ducted a financial investigation, analyzing her spending patterns, to identify her cash for cash transactions (Rose, 4). In the case involving Liu’s use of casinos, financial investigations played a large part in his identification. The Secret Service identified a large influx of Supernotes occurring at Las Vegas casinos via “intelligence reports,” such as CTIRS (U.S., Internal Revenue Manual, 9.5.3.8.3). Once law enforcement agencies identified a place being used to introduce Supernotes, financial analysis of individuals spending cash could help identify who utilizes cash and where. Further investigation of casino player accounts could identify a trove of information. Traditional law enforcement techniques, such as surveillance, could then be applied to identify who was responsible for passing the notes. All of these techniques were used to identify and prosecute Chin Ching Liu (Rose, 5).

An additional forensic financial technique was successfully used in the Smoking Dragon/Royal Charm investigations: asset forfeiture. As previously noted, crimes involving the trafficking and distribution of counterfeit U.S. currency have asset forfeiture provisions – property or property that can be traced to the criminal activity then is subject to forfeiture (U.S., Asset Forfeiture, Appendix A-1). In the joint operations, over $4.5 million in Supernotes were seized along with an additional $40 million in other contraband. More importantly, over $24 million in personal property (cash, real property, jewelry, and vehicles) were forfeited by the suspects (“Operation Smoking Dragon/Dragnal”). Violation of the Title 18 USC 473 (Dealing in Counterfeit Notes or Counterfeit Securities) was among the many charges filed in these cases with asset forfeiture provisions (U.S., DOJ, Office of Public Affairs). Asset forfeiture removes profits from crimes, having a two-fold impact: demotivation to commit criminal activity and the removal of additional funds for investing in future criminal activity. Asset forfeiture played a significant role in these cases and assisted in mitigating Supernote distribution.

The use of financial investigations has a positive impact on the integ-
ration phase of laundering Supernotes. Perpetrators responsible for smuggling and acquired, arenaed, and processed in part through financial investigations. Additionally, profits derived from this activity are identified, seized, and forfeited. This effectively shuts down components of the scheme. Although it hamp-
pers the overall operation, the use of financial investigations did previously not directly impact the production aspect of North Korean counterfeiting. The following case examples explore the abil-
ity of financial forensic investigations to directly impact Supreme production.

Sean Garland is not someone typically associated with North Korean counterfeiting. An Irish citizen, Garland is a political activist in the Irish Republican Army (IRA) and U.S. Republican Party (U.S., Indictment: Garland, 1). According to law enforcement, Garland and his co-
spirators laundered over $1 million in North Korean produced Supernotes throughout the United Kingdom and eastern Europe (Nanos, 6). A large-scale operation, involving authorities in several countries and duped Operation Malak, ultimately brought to justice a number of the individuals involved (“The Super Dollar”). The scheme in Operation Malak is somewhat different from those previ-
ously discussed. Garland, et al appeared to deal directly with North Korean operatives (via connections in Russia) to obtain Supernotes and their method of integration was directly through financial insti-
tutions and money-exchanges (U.S., Indictment: Garland, 8; “The Super Dollar”). This eliminates the need for a middle-man to smug-
gle and resell the notes. It also reduces higher profits for North Korea – it is estimated that the price paid for Superdollars in this case was approximately fifty dollars per face value dollar (i.e. Super Dollar”). The exchange of the bills through money-exchange services, which con-
verted the counterfeit U.S. bills for legitimate bills of the host country facilitated a direct cash for cash transaction. Additionally, the currency obtained and then swapped Supernotes did so throughout many juris-
dictions, from countries in the United Kingdom to former soviet bloc repub-
dics and Russia (U.S., Indictment: Garland, 5). This poses one of the difficulties in using financial investigations in this case: mul-
tiple jurisdictions. Obviously, each country would have varying laws en-
couraging or discouraging currency transactions and laundering money. Jurisdictional differences hampered the use of forensic financial investigations to effectively investigate this scheme. As the countriesSmoking Dragon/Royal Charm, the economic transaction itself was not effectively moved aspects of the crime through various jurisdictions. The countries involved may or may not have mutual treaties with one another or have the same elements to substantiate criminal charges. There would be varying laws and regulations defining money launder-
ring requirements, such as record-keeping requirements for transactions or recording cash exchanges. It is likely this was perpetrated by design or to take advantage of the complexities of varying jurisdictions and differing legal systems. Detrimental Inspector Mark Smith of the Secret Service identified a large influx of Supernotes occurring at Las Vegas casinos via “intelligence reports,” such as CTIRS (U.S., Internal Revenue Manual, 9.5.3.8.3). Once law enforcement agencies identified a place in

The countries involved may or may not have mutual treaties with one another or have the same elements to substantiate criminal charges. There would be varying laws and regulations defining money launder-
ring requirements, such as record-keeping requirements for transactions or recording cash exchanges. It is likely this was perpetrated by design or to take advantage of the complexities of varying jurisdictions and differing legal systems. Detrimental Inspector Mark Smith of the Secret Service identified a large influx of Supernotes occurring at Las Vegas casinos via “intelligence reports,” such as CTIRS (U.S., Internal Revenue Manual, 9.5.3.8.3). Once law enforcement agencies identified a place in

The countries involved may or may not have mutual treaties with one another or have the same elements to substantiate criminal charges. There would be varying laws and regulations defining money launder-
ring requirements, such as record-keeping requirements for transactions or recording cash exchanges. It is likely this was perpetrated by design or to take advantage of the complexities of varying jurisdictions and differing legal systems. Detrimental Inspector Mark Smith of the Secret Service identified a large influx of Supernotes occurring at Las Vegas casinos via “intelligence reports,” such as CTIRS (U.S., Internal Revenue Manual, 9.5.3.8.3). Once law enforcement agencies identified a place in
who either curtailed their dealings with North Korean entities or eliminated them altogether (Lange and Greenlees, 2). According to Brad Balbon (a retired East Asian banking expert), “Because the North Korean leadership placed so many of their foreign exchange eggs in the BDA basket, the sanctions on BDA that prompted the closure of these accounts had an unusually effective impact” (Lange and Greenlees, 2). The use of financial investigations in the BDA affair illustrates their ability to impact Supermote counterfeiting: the U.S. can effectively destroy illicit financial institutions who actively launder Supernote money. By closing off foreign exchange, the U.S. directly impaired the financial sector necessary to spend the fake money. The use of financial investigations to support financial sanctions such as Section 311 directly curtailed North Korea’s ability to manipulate Supernote counterfeit U.S. currency.

The use of financial investigations to place political pressure on North Korea also had significant impact in curtailing their criminal activ- ity, including Supermote production. The U.S. began what it termed the Illicit Activities Initiative (IAI) in late 2001—its focus clearly described by David Asher, “It aimed to undertake the Kim regime’s ability to profit from illicit activities. By compelling the regime’s misuse of the international financial and trading system and threaten- ing its accumulated fortune deposited in overseas banks, the initiative sought to create leverage over Pyongan…” (Asher, 2011, 27). The IAI team ultimately grew to more than 200 people from fourteen U.S. agencies and fifteen foreign governments (Asher, 2011, 29). The IAI was described by Assistant Treasury Secretary James Kelly at a State Department meeting in 2003: “The IAI’s purpose was to pursue North Korea state terrorism in criminal and illicit weapons trading activity, to develop the leverage via law enforcement investigations, Treasury Department designa- tions, partner country liaison and international legal measures to counter, contain, influence and, if needed, apply decisive pressure on the regime’s illicit activities and finances. (Asher, 2011, 35)

The IAI had many facets (some of the previously discussed cases were in part outgrowths of IAI) and the use of financial forensic investigations played a large part in its application. Japan became an important partner on large-scale financial inves- tigations, aimed at curtailing North Korean criminal activity, were initiated by Japanese law enforcement (Asher, 2011, 36). In 2002, Japanese law enforcement conducted an investigation of Asahiaga Bank and ultimately seized it (Asher, 2011, 37). Ashikaga Bank was an important tool for North Korea as it was the only Japanese finan- cial institution with a North Korean correspondent account which allowed financial remittances from Japan (Asher, 2011, 37). Japan’s National Tax Administration initiated a tax evasion investigation into the activities of Chosen Soren, a financial institution with a North Korean correspondent account which was responsible for over $200 million dollars in annual financial transactions to North Korea (Asher, 2011, 37). Another IAI related success was the Austrian government’sigation of Golden Star Bank. Golden Star was operated by the North Korean government and functioned as its financial connection to European banks and companies. Golden Star had long been suspected of engaging in criminal acts, including integrating Supernotes and laundering money. Based on Austria’s financial investigations, Golden Star was closed down in 2004 (Asher, 2011, 38). David Asher is clear on the success of the Golden Star investigation. “this was a substantial blow… and likely affected Kim Jong II personally since Golden Star allegedly managed some of his personal fortune” (Asher, 2011, 38).

The use of financial investigations to support IAI operations as previ- ously noted was clearly successful. IAI operations and related cases led to hundreds of arrests and hundreds of millions of cash seizures; tax violation and money laundering charges were utilized by coopera- tive governments to destroy shell companies facilitating North Korean criminal activity (Asher, 2011, 48). However, the IAI ultimately fell victim to political pressure. In fact, the U.S. failed to capitalize on a number of IAI related successes. The U.S. Treasury Department was poised to unveil specific criminal evidence as a part of the Banco Delta Asia action. “This evidence, which has been verified by grand jury, proved beyond any doubt that the North Korean government, all the way up to the highest levels, was at the center of a global crimi- nal conspiracy,” stated David Asher (Asher, 2011, 44). At this time, the U.S. was engaged with North Korea in the Six Party Talks and was attempting to convince North Korea to solidify a nuclear non-pro- liferation agreement. North Korea demanded that the funds frozen at BDA be returned as a condition of resuming these discussions. The U.S. capitulated, the funds seized ($25 million) at BDA were returned to North Korea (Asher, 2011, 46). The IAI was then elimi- nated as the Bush Administration wanted to ensure that North Korea would not participate in the Six Party Talks if the financial pressure continued (Rose-4). The Justice Department did not proceed with charging North Korean officials, as was originally planned, and essen- tially was told to stand-down by the Administration (Asher, 2011, 4 4 – 45). The U.S. reversed course in utilizing financial investigations to contain North Korean criminal activities based on political fear, an action which sent the wrong message to North Korea. “This is not going to go away. They’re not going to stop making super-notes… because they’re desperate,” said Suzanne Hayden, a Justice Depart- ment prosecutor who was assigned to the IAI (Rose-4).

FORENSIC FINANCIAL INVESTIGATIONS CAN SUCCESSFULLY THwart SUPERMOTES

The use of financial forensic investigations to negatively impact North Korean Supermote production was clearly effective in many instances. As noted in Operation Smoking Dragon, financial forensic inves- tigations identified the integration point of Supermotes and further unraveled the various facets of who was responsible for the scheme. Additionally, financial investigations were utilized to facilitate asset forfeiture, dismantle the machinery of a scheme and take the profits away from criminals. In cases involving money laundering and distri- bution of Supernotes. The use of financial forensic investigations to directly impact North Korean production of Supemotes is not quite as obvious; however, it clearly provided significant assistance. Rather than directly attacking the production per se, IAI and related operations utilized financial forensic investigations to dismantle the components necessary to facilitate the counterfeiting scheme. Front companies were identified and eliminated via tax violations and money laundering charges. Complicit financial institutions were identified, investigated, and sanctioned, in some cases destroying the institutions or seriously hampering their ability to conduct business. However effective these measures were, it was unfortunate that the U.S. did not continue to pursue this course of action—the changing political climate in the U.S. led to a reversal of course and clearly less- ened the impact on North Korea. David Asher described the actions taken against Banco Delta Asia as the “…financial shootout round the world for North Korea… bankers global were sent a wake-up call and North Korea quietly lost ready access to hundreds of millions of dollars in bank accounts” (Asher, 2011, 45). The use of forensic financial investigations to disrupt Supermote production and distribu- tion is clear. Financial forensic investigations can be utilized to suc- cessfully combat this and other criminal activity. Gerald McDowell/ AFMLS Chief at the Justice Department further states: “A careful financial investigation can lead from the street dealer to the kingpins. By following the trail of the money and other assets, your financial investigation can reveal the complex structure of major criminal organiza- tions, and it can lead to seizures and forfeitures that will cripple those organizations” (U.S. Asset Forfeiture).

REFERENCES


E-scams: Catching Fraudsters in a Technical World
Katherine Massey

Technology has allowed fraudsters to communicate with each other worldwide. Whether it is the single email sent to a personal email address requesting help to transport goods, or even a spear phishing fraudster claiming to be the vice president of a widely known company, e-scams are becoming more creative. Although e-scam mitigation is not an easy task, the right education and tools can assist to reduce the risk of widespread damage.

The introduction of computers and the Internet has not changed the basic concept of a scam, it has just made it easier for the perpetrators to carry out their fraudulent activities (Eaton and Taylor, 20). The Internet Crime Complaint Center (IC3) has been established to help Internet users report Internet crimes, and offer tips to help users reduce the chance of being caught in an e-scam. In partnership with the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), the IC3’s primary objective is to, "leverage both intelligence and subject matter expert resources" to effectively combat cyber crime (Internet Crime Complaint Center). Other organizations such as Canada's Anti Fraud Centre have been established to help combat cyber criminal activity and reduce the risk of further exploitation.

With the willingness of fraudsters to carry out their crimes on the Internet, it is important for Internet Service Providers (ISPs) and email Service Providers (ESPs) alike to have ways to report the suspected fraudulent activity. Microsoft's Internet Explorer browser has a "safety" icon which may be used to report a suspicious site, as well as, a specialized email address to report potentially fraudulent email communications. Many large-scale ISPs such as Yahoo and AOL have established Feedback Loops (FBL) to segment out suspected spam or scam-ridden communications that have plugged email systems (Getting Into the Feedback Loop). FBL connects as a bridge from a specialized email address to report potentially fraudulent email communications. Many large-scale ISPs such as Yahoo and AOL have established Feedback Loops (FBL) to segment out suspected spam or scam-ridden communications that have plugged email systems (Getting Into the Feedback Loop). FBL connects as a bridge from a recipient's inbox, outward to the source where the email originated. If the recipient elects to report the email communication as spam, then the complaint is documented. A feedback loop may also relay the complaint to the sender, provided it is a trusted email sender such as a large-scale ESP. As spam reports accumulate, the ISPs protect their customers by placing the offending sender's information on a blacklist (Getting Into the Feedback Loop). If a sender's information is blacklisted, it will be blocked and unable to deliver emails until the sender's credentials have been removed from the blacklist or filtered. However, different types of scams may require different types of tools based on the attributes that the scam exhibits.

Phishing is the impersonation of a seemingly legitimate organization. It is an Internet fraud technique that leads to the theft of personal log-in credentials, bank account information, credit cards, and countless other bits of confidential information (What is Phishing?). A phishing communication such as an email usually assumes the identity of a real financial institution, auction site, or other familiar Internet organization. The scam is predicated on an urgent requirement for a victim to access his account and update information due to an unexpected system loss. The fraudster may go on to entrap the victim by informing him that his account will no longer be functional if he does not take immediate action to rectify the problem. (See Figure 1.) By the time officials become aware of what has transpired, the fraudsters have usually removed and relocated their fraud scheme somewhere else within the Internet.

FIGURE 1: eBay Phishing Scam


When analyzing a phishing scam, reviewing the grammatical composition of the email may reveal numerous spelling errors (Gongol). This is attributed to the fact that fraudsters may not be native speakers of the language they are using to write the email. The links within the emails themselves also can indicate a problem. If a link in an email appears to redirect to a different site, then it could mean that the communication is fraudulent. By placing a mouse over the URL listed in an email, the user can review the actual link information. In
phishing emails, these links do not commonly match up but could easily tricked into believing that all ads that run on a trusted site, such as Facebook recently encountered a problematic IKEA malvertising gift card scam, according to ITBusiness.ca columnist, Robert McMillan and Robert X. Cringely. At the peak of the scam, Facebook noticed the fraudster’s Facebook business page gained roughly 5,000 “fans” per hour, until the page was shut down later in the day (McMillan and Cringely). With the inclusion of ads into trusted social media sites, users have become easily tricked into believing that all ads that run on a trusted site, such as Facebook, are legitimate.

An opportunity to fool an unsuspecting victim is not limited to the use of a coupon, as fraudsters have recently started using cell phones to send e-scams. “Smishing” is the term coined for these phishing SMS text messages (Update: $1000 Walmart Gift Card Scam). According to the Better Business Bureau (BBB) of West Florida, there have been fraudsters capitalizing on e-scam activities by sending unsolicited text messages that trick users into believing they have won a gift card from Walmart or Best Buy (“Ignore Those Texts! You Didn’t”) (See Figure 5.) If a cell phone user receives a text from an unknown number that announces that there is a gift card-winner, the BBB encourages users to refrain from engaging with the sender and instead forward the unsolicited spam message to “7726,” which is short-code for “SPAM” (“Ignore Those Texts! You Didn’t”). With the service monitoring the short code “7726”, Groups Speziale Mobile Association (GSM) officially launched a Spam Reporting Service in February 2011. Based on the pilot research conducted

The Nigerian 419 scam, also known as the “Advanced Fee Fraud” is named after the Nigerian Penal code which details finance-based crimes (Blommaert and Omoniyi, 574). According to a study based on the Nigerian 419 scam, it was determined that the scam emails generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam is comprised of four identifying characteristics: 1) primarily generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam, also known as the “Advanced Fee Fraud” (APWG) released phishing statistics bi-annually. During the early part of 2011, the APWG reported that the financial industry was the largest phishing target recording 47%-1% of all reported phishing attacks (APWG). The United States of America remained the most frequently used hosting country for malicious phishing sites by representing 69%-53% of all threats during the first six months in 2011. The United Kingdom, Canada, Egypt, and Germany were the most commonly infected host phishing sites throughout the first half of 2011. For an investigative, the statistics provided aid in identifying the pressure points and determining an appropriate action plan to dismantle phishing scams. By carefully reviewing statistics and trends, an organization may be able to uncover and successfully mitigate other potential problems that may need immediate attention before they escalate to large scale scams.

To help combat phishing attacks, the Anti-Phishing Working Group (APWG) actively works to educate the public about phishing attacks and how to prevent them. The APWG releases phishing statistics bi-annually. During the early part of 2011, the APWG reported that the financial industry was the largest phishing target recording 47%-1% of all reported phishing attacks (APWG). The United States of America remained the most frequently used hosting country for malicious phishing sites by representing 69%-53% of all threats during the first six months in 2011. The United Kingdom, Canada, Egypt, and Germany were the most commonly infected host phishing sites throughout the first half of 2011. For an investigative, the statistics provided aid in identifying the pressure points and determining an appropriate action plan to dismantle phishing scams. By carefully reviewing statistics and trends, an organization may be able to uncover and successfully mitigate other potential problems that may need immediate attention before they escalate to large scale scams.

The Nigerian 419 scam, also known as the “Advanced Fee Fraud” is named after the Nigerian Penal code which details finance-based crimes (Blommaert and Omoniyi, 574). According to a study based on the Nigerian 419 scam, it was determined that the scam emails generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam is comprised of four identifying characteristics: 1) primarily generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam, also known as the “Advanced Fee Fraud” (APWG) released phishing statistics bi-annually. During the early part of 2011, the APWG reported that the financial industry was the largest phishing target recording 47%-1% of all reported phishing attacks (APWG). The United States of America remained the most frequently used hosting country for malicious phishing sites by representing 69%-53% of all threats during the first six months in 2011. The United Kingdom, Canada, Egypt, and Germany were the most commonly infected host phishing sites throughout the first half of 2011. For an investigative, the statistics provided aid in identifying the pressure points and determining an appropriate action plan to dismantle phishing scams. By carefully reviewing statistics and trends, an organization may be able to uncover and successfully mitigate other potential problems that may need immediate attention before they escalate to large scale scams.

The Nigerian 419 scam, also known as the “Advanced Fee Fraud” is named after the Nigerian Penal code which details finance-based crimes (Blommaert and Omoniyi, 574). According to a study based on the Nigerian 419 scam, it was determined that the scam emails generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam is comprised of four identifying characteristics: 1) primarily generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam, also known as the “Advanced Fee Fraud” (APWG) released phishing statistics bi-annually. During the early part of 2011, the APWG reported that the financial industry was the largest phishing target recording 47%-1% of all reported phishing attacks (APWG). The United States of America remained the most frequently used hosting country for malicious phishing sites by representing 69%-53% of all threats during the first six months in 2011. The United Kingdom, Canada, Egypt, and Germany were the most commonly infected host phishing sites throughout the first half of 2011. For an investigative, the statistics provided aid in identifying the pressure points and determining an appropriate action plan to dismantle phishing scams. By carefully reviewing statistics and trends, an organization may be able to uncover and successfully mitigate other potential problems that may need immediate attention before they escalate to large scale scams.

The Nigerian 419 scam, also known as the “Advanced Fee Fraud” is named after the Nigerian Penal code which details finance-based crimes (Blommaert and Omoniyi, 574). According to a study based on the Nigerian 419 scam, it was determined that the scam emails generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam is comprised of four identifying characteristics: 1) primarily generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam, also known as the “Advanced Fee Fraud” (APWG) released phishing statistics bi-annually. During the early part of 2011, the APWG reported that the financial industry was the largest phishing target recording 47%-1% of all reported phishing attacks (APWG). The United States of America remained the most frequently used hosting country for malicious phishing sites by representing 69%-53% of all threats during the first six months in 2011. The United Kingdom, Canada, Egypt, and Germany were the most commonly infected host phishing sites throughout the first half of 2011. For an investigative, the statistics provided aid in identifying the pressure points and determining an appropriate action plan to dismantle phishing scams. By carefully reviewing statistics and trends, an organization may be able to uncover and successfully mitigate other potential problems that may need immediate attention before they escalate to large scale scams.

The Nigerian 419 scam, also known as the “Advanced Fee Fraud” is named after the Nigerian Penal code which details finance-based crimes (Blommaert and Omoniyi, 574). According to a study based on the Nigerian 419 scam, it was determined that the scam emails generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam is comprised of four identifying characteristics: 1) primarily generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam, also known as the “Advanced Fee Fraud” (APWG) released phishing statistics bi-annually. During the early part of 2011, the APWG reported that the financial industry was the largest phishing target recording 47%-1% of all reported phishing attacks (APWG). The United States of America remained the most frequently used hosting country for malicious phishing sites by representing 69%-53% of all threats during the first six months in 2011. The United Kingdom, Canada, Egypt, and Germany were the most commonly infected host phishing sites throughout the first half of 2011. For an investigative, the statistics provided aid in identifying the pressure points and determining an appropriate action plan to dismantle phishing scams. By carefully reviewing statistics and trends, an organization may be able to uncover and successfully mitigate other potential problems that may need immediate attention before they escalate to large scale scams.

The Nigerian 419 scam, also known as the “Advanced Fee Fraud” is named after the Nigerian Penal code which details finance-based crimes (Blommaert and Omoniyi, 574). According to a study based on the Nigerian 419 scam, it was determined that the scam emails generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam is comprised of four identifying characteristics: 1) primarily generated by a fraudster tend to follow a similar flow. The Nigerian 419 scam, also known as the “Advanced Fee Fraud” (APWG) released phishing statistics bi-annually. During the early part of 2011, the APWG reported that the financial industry was the largest phishing target recording 47%-1% of all reported phishing attacks (APWG). The United States of America remained the most frequently used hosting country for malicious phishing sites by representing 69%-53% of all threats during the first six months in 2011. The United Kingdom, Canada, Egypt, and Germany were the most commonly infected host phishing sites throughout the first half of 2011. For an investigative, the statistics provided aid in identifying the pressure points and determining an appropriate action plan to dismantle phishing scams. By carefully reviewing statistics and trends, an organization may be able to uncover and successfully mitigate other potential problems that may need immediate attention before they escalate to large scale scams.
In Phase 1, the fraudster places ads on internet dating and social media sites to locate victims. Based on Garrett’s research, the Russian Dating Scam targets hopeful individuals seeking job opportunities in a tough economy. The scam captures email addresses of individuals who are seeking relationships with foreign males. The fraudster targets emails of young females that can use the e-scammers as “bait.” The manipulation begins with media sites to locate victims. Advertisements include pictures, brief profiles and contact details to serve as “bait.” The manipulation begins with media sites to locate victims. Advertisements include pictures, brief profiles and contact details to serve as “bait.”

In close relation to other world-wide e-scams, the Russian Dating Scam often utilizes the tactics of post-grabbing, broken English, and the bait of a lonely victim looking for love (Garrett). Though the scam stereotypically involves using an alias of a female between the ages of 18 to 45 years old seeking a foreign male love, the e-scammers can take on many other variations. (Garrett). More often than not, the fraudster searches for image online of young females that they can use as a default profile picture. According to Elena Garrett, author of the Russian Detective website, the motives of a Russian Dating Scam can vary considerably. The fraudster typically asks for one or more of the following items: passport or visa, money for travel, fines, bail, medical expenses, or transfer fees, and or gifts (clothing, cellphones, jewelry). (Garrett).

The Job Recruiting Scam borrows elements from both the Nigerian 419 Scam and the Russian Dating Scam. The Job Recruiting Scam captures hopeful individuals seeking job opportunities in a tough economy. The employment scam claims to seek qualified applicants for work for a company offering a highly competitive salary (“Employment Scams”). The Scam Detectives provide four key points to help an unsuspecting victim determine if the email they received is genuine, or the result of an elaborate e-scam. A legitimate company will not reach out to a person seeking a job opportunity unless the individual contacted the company beforehand. A legitimate email sent from an honest recruiting agency includes more details than simply an email address to contact them. Much like other scams, the domain of a legitimate company would be used in the email address, rather than a free web-based ISP such as live.com. Any mention of a third party processing services to service invoices is highly suspicious, and should raise concerns regarding the legitimacy of the company (“Employment Scams”).

The online adult entertainment industry is a lucrative business as it is estimated that users spend approximately $3.5 billion on adult materials on the Internet every second (Ropelato, “Internet”). Fraudssters within the industry have commonly practiced a scam referred to as “Porn-Napping.” This includes hijacking a domain name that has not been renewed by the original owner, and loading it with adult materials (Ropelato, “Tricks”). Another attempt to deceive and entice internet users is known as a Russian Dating Scam, or “FalsoLove.com.” In this e-scam, fraudsters manipulate mainstream search engines by using non-suspect themes and language on their webpages to trick the search engine into assuming that the site is clean (Ropelato, “Tricks”). By using redirecting links or multiple sites linked to one another, the fraudster sends the user through several different sites before ultimately leading them to the adult entertainment site. Depending on which tactics are used, the user may find it difficult to escape as a result of redirects and ads implanted in the website or even in the unsuspecting victim’s computer (Ropelato, “Tricks”).

According to the Canadian Anti Fraud Centre, there have been multiple reports from consumers that were tricked into believing that their computers were illegally associated with a child pornography ring. (Garrett). This involves sending emails to anyone they suspect may be engaging in fraudulent activity, and try to get them to view a malicious attachment. Users that their computers will remain locked for further review unless they agree to pay $100 through a third party wiring service to have their computer unlocked (Scamware scam warning). Also known as “Scamware,” these types of tactics are used to target innocent victims due to the shock value and taboos nature of the content that has been associated with their computers. The Anti Canadian Fraud Centre issues tips to computer users to reduce the associated risk of this scam, but strongly encourages users to scan their computers for viruses and malware that could have been transferred via an infected email communication.

E-scams do not always lead to victimization by stealing money and goods, sometimes the victimization may mean that a user’s computer participates in the e-scam, and is controlled by the fraudster once it is infected with malware. According to statistics released by Damballa, an advanced threat protection provider, it is estimated that 40% of computers of the 800 million computers connected to the Internet are potentially engaging in botnet activity on a daily basis. A botnet takes an e-scam a step further, as an infection can start out as a download on a website or an email sent to a user. In 2008, an e-scam was created, spreading via the mail of an actor's Hawk Logo, and included a link that supposedly would lead the user to a police report regarding the truth behind Ledger’s death (Acohido and Swartz). If the user clicked on the link, the machine became infected and enabled the fraudsters to push out email spam through the Mega-D botnet, which mostly distributed male-enhancement spam.

The Blahsack-based botnet infiltrated the Internet and was implicated in the infection of over 600,000 computers on April 9, 2012 (“Flashback Cleanup Still Underway”). Primarily used as a means to further click-fraud profits, the botnet is difficult to dismantle, as all users are not aware that they need to run updates and use malware removal tools in order to counter the botnet damage (Greenberg). Mac users did not require installed anti-virus protection, as infections were few and far between until recently (Rubinstein). In discussing Windows OS exploit of Conficker worm in 2008, PC Magazine’s Security Watch reporter Neil Rubenstein has attributed the success of the botnet to the average Mac user’s false sense of security, complacency and lack of the appropriate anti-virus protection. When proving the legitimacy of an email sender source, Internet users need a process by which to delineate reputational data to reduce the chances of e-scammers reaching a user’s inbox. According to the Online Trust Alliance (OTA), email is the primary method of communication for both personal and business matters (“Email Authentication Rates Rise”). The OTA estimates that 95% of emails consist of some sort of spam, phishing, or malware. From the perspective of an ISP or an IRI utilizing technology such as the DomainKeys Identified Mail (DKIM) places the burden of responsibility on the organization that is sending an email communication to a user’s inbox (“Introduction”). By authenticating an email, it allows the recipient’s service to review the reputational past history of the sender address, and make a decision about sending the communication directly to the inbox, to a junk folder, or blocking the communication altogether (“Introduction”) (See Figure 6.).

The development of a similar technology within the field transported when Microsoft released their own email authentication process, Sender ID Framework (SIDF) (Sender ID Framework Overview). (See Figure 7.) SIDF was created by Microsoft as a way to stop security problems arising from spam, phishing, and other potentially malicious communications from reaching the user's inbox. Similar to DKIM, Microsoft verifies that email communications have legitimate headers and determines the reputation of the authenticated address to see if there have been any recorded information regarding abuse complaints or spam. Figure 7 illustrates the standard protocol of an email that is sent through the SIDF process to check the validity of the message prior to reaching the inbox.


Sender ID Framework (SIDF) (Sender ID Framework Overview). (See Figure 7.) SIDF was created by Microsoft as a way to stop security problems arising from spam, phishing, and other potentially malicious communications from reaching the user’s inbox. Similar to DKIM, SIDF checks to see if there have been any recorded information regarding abuse complaints or spam. Figure 7 illustrates the standard protocol of an email that is sent through the SIDF process to check the validity of the message prior to reaching the inbox.


Sender ID Framework (SIDF) (Sender ID Framework Overview). (See Figure 7.) SIDF was created by Microsoft as a way to stop security problems arising from spam, phishing, and other potentially malicious communications from reaching the user’s inbox. Similar to DKIM, SIDF checks to see if there have been any recorded information regarding abuse complaints or spam. Figure 7 illustrates the standard protocol of an email that is sent through the SIDF process to check the validity of the message prior to reaching the inbox.

In order to combat cyber crime, the onus is on all parties who use an electronic device such as a computer or a cell phone to access the Internet. As fraudsters become more creative with their e-scams tactics, it is important that no user is too comfortable with their surroundings while checking their email, or surfing the web. New tools and product suites continually enter the market in an attempt to "one-up" the bad guys, and keep them away from legitimate operations. The more a consumer is aware of fraud, and how it may impact their daily lives, the less success fraudsters will have when running their illegal operations.

REFERENCES


INTRODUCTION

During the past two years, technology has helped society perform some of the most challenging tasks faster than was previously possible. While computers have helped law abiding citizens, they have also helped criminals and terrorists commit their crimes with the same level of ease. One technology, which is helping criminals, terrorists, and regular citizens alike, is steganography: the method of concealing electronic files in other files. Steganography has given people a means to pass information across a public medium, such as the Internet, while avoiding detection from those who should not view the file. Despite being in use for over two thousand years, steganography has adapted to current trends in technology thus continuing to provide a method of concealing data.

HISTORY OF STEGANOGRAPHY

Steganography is not a new technology. In fact, it dates back to the time of the Roman Empire and the ancient Greeks. As Tom Kellen2 writes:

"The Greek historian Herodotus recorded one of the earliest recorded uses of steganography. He tells of how one of his countrymen sent secret messages by writing them on the wooden base of wax tablets. The wax on top was blank, and the tablet was thought not to contain any information. (Kellen)"

In another paper submitted to the SysAdmin, Audit, Network, Security (SANS) Institute (one of the most trusted and by far the largest source for information security in the world), author Stephen Lau provides additional background into steganography. Law explains, "A Roman General shaved the head of a slave and tattooed a message on the shaved head. After the hair grew back, the slave delivered the message by walking to the message's intended recipient who subsequently shaved the slave's head to reveal the hidden message." (La)

Steganography was even used during World War II. Soldiers on both sides, Allied and Axis, used various methods to communicate discreetly with each other. Records show that the soldiers used invisible "ink" to write battle plans so as to pass them to each other undetected by the other side. This invisible ink was actually milk, fruit juice, or other liquids that were dry clear but darken when heated. Soldiers would write messages and battle plans on pieces of paper and carry these concealed documents without fear of being caught by enemy soldiers. If the courier would happen to be captured, the plans would likely show distortion, signaling that something may be hidden inside. However, just selecting an unintended carrier file that is larger than the intended payload can still prove problematic. While a carrier file that is only slightly larger than the payload will have more room to conceal the hidden data, the amount of space is still limited. The ideal carrier file is significantly larger than the payload since it will have ample storage space to conceal any data that is passed through it. Another benefit to a carrier file with a significantly larger size is that once the file size increases due to the payload, the new size will be much more noticeable.

TRADITIONAL DETECTION OF STEGANOGRAPHY

"Steganography relies on the fact that the human senses are inadequate when compared to analysis performed by machines or even in fact the senses of other animals of the earth." (McGill) Most people who choose to send information covertly across a digital medium such as the Internet use some form of cryptography. Cryptography is defined as the process of creating, communicating in, and deciphering secret writings or messages. This however can be a signal to anyone watching that something is happening on that connection. Steganography transfers information across a connection so that anyone monitoring the link will not be able to detect what is being sent. As Dr. Cole states, there is no point in hiding data if someone can figure out how and where the data is hidden. Steganography is designed to make the hidden data hard to detect by disguising it in such a way that there is little change to the properties of the hidden file. (Cole)

Steganalysis, the art of detecting the use of steganography, is very tedious and difficult. The easiest way to determine if steganography has been used is if steganography related programs are installed on the target computer. As most people are not aware of steganography, there is little chance that a normal user would install any of these programs. Another method of steganalysis involves utilizing computer forensics for detection. Computer forensics can be used to "hunt down evidence by detecting damaged or hidden files and opening password-protected or encrypted files." (Cole) According to Pierre Richet in his paper titled "Detecting Hidden Information with Computer Forensic Analysis" (2003), there are multiple forensic methods of detecting steganography. These methods include:

- Stego-only attack – Only the stego-object is available for analysis. For example only the carrier-header and steganographic information are available. (Richet)
- Known cover attack – The original cover-object (the file that contains the hidden data, also called carrier file) is compared with the stego-object and pattern differences are detected. For example, the original image and the image containing the hidden information are available and can be compared. (Richet)
- Chosen stego attack – The steganography tool (algorithm) and stego-object are known. For example, the software and the stego-carrier and hidden information are known. (Richet)

Most forensic tools also have the option to scan files for a signature, which may indicate the use of steganography. A signature is a mathematical method of determining the authenticity of a digital message or document. All software has its own unique digital signature therefore a forensic tool performing a signature scan may be able to detect the carrier files if the signature list is current. In addition to signature detection, some programs can detect steganography, although along so is difficult. The first step in detection is to locate files with hidden text, which can be done by analysing patterns in the images and changes to the color palette. (Graves) To combat forensic detection of steganography, author Stephen Lau writes:

"In recent years, more sophisticated techniques have evolved, specifically to defeat most standard methods of detecting steganography. These involve analysing the image prior to embedding the message to determine its statistical properties. By locating redundant bits of an image and probabilistically replacing the bits with new information, one can defeat most statistical analyses. In addition, by subsequently modifying other portions of the image, one can recreate the "statistical" footprint of the original unmodified image that can thwart most attempts at statistical analysis. (La)"

Figure 1 illustrates one method by which a forensic analyst would be able to detect the use of steganography; but only if the original file is known. Every digital file has a hash value which remains constant as the file remains unchanged. A hash value is a mathematical representation of the data contained in the file. Generally speaking, hash values are unique to each file and are difficult to duplicate on another file. Once a change is made to the file, the hash value will also change, thus reflecting an alteration to the document. In Figure 1, the hash value in the top field is from the original file and the hash to compare field is the file that has been altered by steganography.

Impact of Steganography on a Forensic Investigation

Ryan Spishock, CISSP
officially released the New Technology File System (NTFS) to home users. NTFS provided users with the benefits of being able to support higher capacity storage devices as well as a higher level of security by providing disk encryption and recoverability as well as other methods of built-in security.

NTFS features alternate data streams (ADS) which function in a similar manner as steganography. ADS allows a hidden file to be created within a legitimate file; these hidden files do not appear in a directory listing as a legitimate file would. (Gross 114-115) Each stream associated with a file has its own allocation size, actual size, and valid data length:

- The allocation size is the amount of disk space reserved for a stream.
- The actual size is the number of bytes used by a caller.
- The valid data length (VDL) is the number of bytes initialized from the allocation size for the stream. (“Microsoft”)

As shown in Figure 2, every file has several components that provide various pieces of information about the individual file. In addition to file attributes, files stored on an NTFS system also contain a listing of all security restrictions for that file. NTFS also adds streams to each file. A stream is a sequence of bytes containing all of the data written to the file as well as various pieces of information used by the system to store and retrieve the file.

**FIGURE 2**

Source: http://www.techken.com/docs/articles/alternate-streams.php.html

With traditional steganography, when a file is written to a carrier file, the size of the carrier file will increase to compensate for the added data. With ADS, the hidden data is not combined with the carrier file by the same method used in steganography. Instead, the hidden data is written to an alternate data stream that is ignored by the file system. Figure 3 shows the size of a file called test.txt. Figure 4 shows the file size of test.txt that also contains a file called hidden.txt; the size of both files is 15 bytes.

**FIGURE 3**

As shown in Figure 2, every file has several components that provide various pieces of information about the individual file. In addition to file attributes, files stored on an NTFS system also contain a listing of all security restrictions for that file. NTFS also adds streams to each file. A stream is a sequence of bytes containing all of the data written to the file as well as various pieces of information used by the system to store and retrieve the file.

**FIGURE 4**

**DETECTING ADS**

Because of the manner in which ADS hides data, it is undetectable by traditional forensic tools. Figure 5 is a screenshot from Forensic Toolkit (FTK) Imagery that shows the contents of test.txt after hidden.txt was added to it. FTK is only able to detect the actual contents of the file, i.e. the string of text “This is a test” but not the hidden string “This should be hidden.”

**FIGURE 5**

Since ADS are undetectable by standard forensic methods, a variety of tools have been created which are able to detect if anything is hidden within a file using data streaming. Figure 6 shows the output of one ADS tool called lns that detects the presence of a file called hidden.txt within a legitimate file; these hidden files do not appear in a directory listing as a legitimate file would. (Gross 114-115) Each stream associated with a file has its own allocation size, actual size, and valid data length:

- The allocation size is the amount of disk space reserved for a stream.
- The actual size is the number of bytes used by a caller.
- The valid data length (VDL) is the number of bytes initialized from the allocation size for the stream. (“Microsoft”)

As shown in Figure 2, every file has several components that provide various pieces of information about the individual file. In addition to file attributes, files stored on an NTFS system also contain a listing of all security restrictions for that file. NTFS also adds streams to each file. A stream is a sequence of bytes containing all of the data written to the file as well as various pieces of information used by the system to store and retrieve the file.

**FIGURE 2**

Source: http://www.techken.com/docs/articles/alternate-streams.php.html

With traditional steganography, when a file is written to a carrier file, the size of the carrier file will increase to compensate for the added data. With ADS, the hidden data is not combined with the carrier file by the same method used in steganography. Instead, the hidden data is written to an alternate data stream that is ignored by the file system. Figure 3 shows the size of a file called test.txt.

**FIGURE 3**

As shown in Figure 2, every file has several components that provide various pieces of information about the individual file. In addition to file attributes, files stored on an NTFS system also contain a listing of all security restrictions for that file. NTFS also adds streams to each file. A stream is a sequence of bytes containing all of the data written to the file as well as various pieces of information used by the system to store and retrieve the file.

**FIGURE 2**

Source: http://www.techken.com/docs/articles/alternate-streams.php.html

With traditional steganography, when a file is written to a carrier file, the size of the carrier file will increase to compensate for the added data. With ADS, the hidden data is not combined with the carrier file by the same method used in steganography. Instead, the hidden data is written to an alternate data stream that is ignored by the file system. Figure 3 shows the size of a file called test.txt.

**FIGURE 3**

As shown in Figure 2, every file has several components that provide various pieces of information about the individual file. In addition to file attributes, files stored on an NTFS system also contain a listing of all security restrictions for that file. NTFS also adds streams to each file. A stream is a sequence of bytes containing all of the data written to the file as well as various pieces of information used by the system to store and retrieve the file.

**FIGURE 2**

Source: http://www.techken.com/docs/articles/alternate-streams.php.html

With traditional steganography, when a file is written to a carrier file, the size of the carrier file will increase to compensate for the added data. With ADS, the hidden data is not combined with the carrier file by the same method used in steganography. Instead, the hidden data is written to an alternate data stream that is ignored by the file system. Figure 3 shows the size of a file called test.txt.

**FIGURE 3**

As shown in Figure 2, every file has several components that provide various pieces of information about the individual file. In addition to file attributes, files stored on an NTFS system also contain a listing of all security restrictions for that file. NTFS also adds streams to each file. A stream is a sequence of bytes containing all of the data written to the file as well as various pieces of information used by the system to store and retrieve the file.

**FIGURE 2**

Source: http://www.techken.com/docs/articles/alternate-streams.php.html

With traditional steganography, when a file is written to a carrier file, the size of the carrier file will increase to compensate for the added data. With ADS, the hidden data is not combined with the carrier file by the same method used in steganography. Instead, the hidden data is written to an alternate data stream that is ignored by the file system. Figure 3 shows the size of a file called test.txt.
In relation to steganography, the file signature of the payload file is which is the signature for all .jpg files. (Kessler) still contain a file signature of “FF D8 FF E0 xx xx 4A 46 49 46 00” require file extensions. Altering the file’s extension does not alter the file signature alone and determine what software is required to open the file. The file signature is a small block of hexadecimal code used to connect to the system. In addition to searching obscure locations for evidence, a forensic investigator would look for that would signal that data is hidden and national interests from terrorist activities. It would also take away the one place that criminals can hide to avoid detection. Presenting a case to court based on steganographic evidence can be very difficult since it is not a well-known technology. However, including a steganalyst on staff to act as an expert witness to the courts can help increase the chance of successfully processing a suspect.

IMPACT ON AN INVESTIGATION

Investigators are trained to search obscure locations during an investigation in an attempt to locate evidence that will either prove or disprove a suspect’s guilt. Typically, there are various signs that an investigator would look for that would signal that data is hidden using these techniques. For example, if an investigator has a drive that appears to be empty, they may try to recover the deleted file system using common forensic tools. The same would apply with a hard drive labeled with a capacity of 1 TB but only shows 500 GB when connected to the system.

In addition to searching obscure locations for evidence, a forensic investigator will also perform signature analysis on files to determine if tampering has occurred. On Windows based systems, files are specified by their extension (.exe, .pl, .pdf, etc.). Windows uses these extensions to load the correct software when the user calls for that specific file to open. It should be noted that while files on UNIX based systems might also show file extensions, the operating system does not require them. UNIX based systems are able to look at the file signature alone and determine what software is required to open the file.

The file signature is a small block of hexadecimal code used to determine the type of file. This is why UNIX based systems do not require file extensions. Altering the file’s extension does not alter the signature, therefore, changing a .jpg image to a Word document will still contain a file signature of “FF D8 FF E0 xx xx 46 49 46 00” which is the signature for .jpg files. (Reader)

In relation to steganography, the file signature of the payload file is broken down and added to several least significant bits (LSB) of the carrier file. Therefore, performing signature analysis on a carrier file will only show the signature of the carrier and not the payload. Masking the file signature by embedding it within the carrier file is an easy method to avoid detection by a forensic investigator.

Forensic tools such as WinHex have the ability to compare multiple files to determine if differences exist. Figure 9 shows the comparison of two files, one of which was the image on the top left of Figure 8 and the other was the image on the top right. As Figure 9 shows, WinHex was unable to locate any differences between the two images with the exception of the size of the file. During an investigation, if the forensic investigator found these two files and received the same output from tools such as WinHex, the next logical step would be to run a steganalysis tool such as StegDetect or StegJHunt on the images to attempt to locate the hidden content, especially if steganography tools were located on the evidence drive.

![Figure 9](image.png)

**FIGURE 9**

While forensic tools are unable to detect steganographic content on their own, these tools will allow the investigator to build hash files from files that are known to contain hidden content. Once steganographic content has been located, the investigator can use tools such as Forensic Toolkit to generate an exportable list that includes the hash values for all of the carrier files. These lists can be used during future investigations to locate copies of the original carrier file that may have been shared.

CONCLUSION

As stated in “Steganalysis Detecting Hidden Information with Computer Forensic Analysis”, Although steganography is becoming more advanced, it is still a science that is not well known. In use on the Internet is certainly promising. That is why law enforcement authorities must continually stay abreast of this technology, because there will always be some new program to hinder their efforts. (Richer) Criminals are constantly finding new methods to stay ahead of law enforcement and avoid detection. While not everything on the Internet is what it seems to be, the possibility of these images containing plans of mass destruction or other illegal content is increasing daily. Traditional forensic tools provide investigators with the ability to create hash sets that can be used to detect steganographic content, however, the changes to the carrier files are made at such a low level, that the forensic tools are not able to detect the hidden content on their own. By incorporating steganalysis tools as part of a forensic investigator’s professional toolkit, the investigator will be better prepared to detect hidden content during an investigation.

REFERENCES

INTRODUCTION
In 2005, American charities took in $260 billion in cash donations with religious groups receiving the greatest portion at $93.3 billion (Barrett, Johnson, and Croosing, 2005, p.29) It is estimated that in 2010, religious leaders will commit $34 million in fraud (Bama Group). To complicate the fraud issue, 80 percent of fraud cases are not investigated by law enforcement. In most cases, religious organizations preferred to avoid public media attention (Barrett et. al., 2001). Thus, it is difficult to establish the extent of current fraud in a quantitative amount. However, it is clear that fraud is a problem in the Christian church and needs to be addressed.

Fraud in the American church is not limited to the 21st century.

Fraud has always been an issue for all religious organizations. However, it was during the early 1970s and the late 1980s, when this issue was brought to the attention of the American people due to the growth of television evangelism. Select evangelical leaders had million dollar salaries, drove luxury cars, traveled in private jets and lived in lavish homes from Malibu to Miami. Although prime examples of this extravagant lifestyle were James and Tammy Faye Bakker, other religious leaders including those in Jewish and Muslim organizations have also participated in fraudulent activities. (Schmidt). For example, in 2009, Rabbi Saul Kassin was arrested for a $3 million money-laundering scheme (NY Times). The following year, Salman Ibrahim swindled hundreds of Chicago Muslims out of $30 million using a Ponzi Scheme (Tami).

Fraudsters have one obsession: becoming rich through swindling people who unknowingly place their faith (and hard-earned money) in fraud schemes. The purpose of this paper is to help prevent religious organizations from becoming victims of financial crimes. It is this writer’s position that the total dollar loss is traceable to a minute amount of financial activities conducted within a religious organization. Thus, by developing financial controls, which target those specific areas, these organizations will reduce the risk of becoming fraudulent victims. This paper will provide a basic explanation of fraud schemes.

Fraud schemes can be categorized as: Corruption, Asset Misappropriation, and Fraudulent Statements. Of these three categories, Asset Misappropriation occurs most frequently Corrupting, Asset Misappropriation, and Fraudulent Statements. Of these three categories, Asset Misappropriation occurs most frequently

For separation of duties to exist, all employees must follow the same procedures and process. Any employee entering the amount on the deposit slip, records the deposit in the organization’s internal-control structure. For separation of duties to exist, the employee entering the amount on the deposit slip, records the deposit in the organization’s internal-control structure.

The third task for the Board is to perform regular reviews of financial transactions. The policy should include: review of posted transactions in the accounting system, access to source documents, and evidence of authorizing signatures. In addition, all account reconciliations must follow the same procedures and process. The Board members must review these documents for compliance with accounting procedures. The fourth task for the Board is to ensure proper separation of duties within the organization. Separation of duties is the cornerstone of the organization’s internal-control structure. For separation of duties to occur, it is essential that authorizations of transactions, transaction recording and custody of assets be kept separate. A typical example of unsegregated duties is when the treasurer counts the weekly, enters the amount on the deposit slip, records the deposit in the accounting system, and reconciles the bank account. The three duties: depositing, recording, and reconciling should be divided among three people. The Board’s fifth task is to review and approve all related party transactions. The organization’s membership typically includes professionals, business owners, and skilled laborers who are willing to volunteer their time and expertise. Therefore, when religious organizations are in need of goods or services, they may turn to their members. While these types of related-party transactions may be in the church’s advantage, there are cases in which a related-party transaction results in a transfer of wealth from the organization to the individual. Such related-party transactions must be fully disclosed, verified that the transactions are at fair market value, approved by the Board, and upheld by a vote of the membership.

The sixth task is to ensure the organization has sound human resource practices. Most organizations want to hire ethical people. However, over time people can become corrupt. The challenge for a church is to hire ethical people and establish a working environment bound by ethics and integrity. The size and longevity of a fraud is directly related to the staff members’ tenure. Religious organizations must establish best practices in their staffs’ lifecycles to include hiring, retention, and termination of staff members. The hiring process should be used to screen out potential employees who might pose a greater risk for financial fraud. Four basic employment screens are beneficial: criminal background checks, public records searches, verifications of qualifications, and home visits. During the staff members’ tenures, the church should have an enforced leave policy, annual performance evaluations, compensation adjustments, a grievance process, professional development opportunities, and exit interviews.

The final task is to ensure an ethical workforce stays ethical. The religious organization can accomplish this by placing outside pressure on the staff members. In the 2010 Survey of Fraud, the ACFE found that anonymous hotlines had the greatest impact in detecting fraud (Association of Certified Fraud Examiners, 2010, pg. 17). Thus, an anonymous tip line will assist in the deterrence of fraud by creating the potential fraudsters to speculate whether their activities will be noticed and/or reported and by serving as an outlet for those suspecting fraud. In addition to a tip line, the Board should consider bond insurance.

Bond insurance provides the Board with a quick and easy method to deter fraud and manage actual losses. With bond insurance, staff members are not only accountable to the Board and membership, they are accountable to an outside entity which has no personal relationship to them and will litigate to recover losses. These types of insurance bonds are available to religious organization through a local insurance broker. The size of the organization and purpose of the bonds will dictate the type of bonds that can be chosen.

FINANCIAL CONTROLS
As noted previously, the ACFE has identified three categories of fraud: Corruption, Asset Misappropriation, and Fraudulent Statements. Of these three categories, Asset Misappropriation occurs most frequently with cash schemes as the most common (Association of Certified Fraud Examiners, 2006, pg. 12.) Thus, the internal control structure within religious organizations should focus on cash transactions and documentation i.e. cash receipts, cash disbursements, and expense reporting. By adopting such an approach, the Board will deter the majority of financial losses due to fraud.
CASH RECEIPTS

There are six schemes for cash receipt frauds: skimming, lapping, write-off of accounts receivable, unauthorized credits, unrecorded sales, and theft of donated merchandise. The most common of these schemes is skimming, therefore, internal controls for cash receipts in religious organizations should be focused on those areas vulnerable to skimming.

Skimming schemes involve the theft of donated funds prior to the funds being documented in the accounting records. The donated funds are usually in the form of cash, checks, or credit cards. In religious organizations, the most common are cash donations or checks. Obviously, cash contributions are the most vulnerable to skimming. Thus, the control mechanism will be based on the regulation of cash.

Some methods used to regulate cash are:

- Use offering envelopes for donations.
- Donation envelopes serve two purposes: 1) create a source record of the donation, and 2) protect the cash until a bank deposit slip is completed. The envelopes should be kept as source documentation.
- Control collections
- The collection committee should select at least two or more unrelated people for collecting and recording the cash receipts. After the collection process is completed, the receipts should be taken to a secure location to be counted, recorded in the accounting system, with a bank deposit slip and a collection report completed in their parts. The collected funds (with one copy of the bank deposit form) are secured in a locked bank deposit bag and placed in a safe or other locked container until deposit. The collection committee should keep and file a copy of the collection report. In addition, many religious organizations receive cash through religious classes, rental of facilities, preschool programs, and other activities. The cash receipts for these revenue generating activities should follow the same procedures.

- Restictively endorse all checks during initial counting process.
- During the cash receipt process, the checks should be restictively endorsed. Usually, a person stamps the back of the check "for deposit only." In a religious organization, a pre-engraved rubber stamp should be provided to the members performing the cash receipt functions. All checks received should be stamped during the tallying of the collection.
- A bank drop box should be utilized for cash receipts.

Once the collection process is completed, the cash receipts should be deposited as soon as possible to decrease the opportunity for theft and to increase promptness of the check-cashing process in order to avoid issues with bad checks. The preferred technique is the utilization of an after-hours bank drop box. If the local bank does not have an after-hours drop box, the religious organization should make the deposits early on the next business day.

- Segment the authorization, recording, and reconciliation elements of the cash receipt process
- As stated earlier, separation of duties is the keystone of the organization’s internal control structure. It is essential to appoint two or more unrelated parties to perform the entire cash receipt function. During the collection process, two source documents are created: a deposit slip in three parts and a collection report in four parts. These documents are fundamental to the verification of received funds and the reconciliation process. Optimally, after the deposit, the collection committee should have three copies of the collection report and two remaining copies of the deposit slip. The committee should send a copy of each document to the (A) Treasurer and a copy to the (B) Board.

A. The Treasurer should enter the cash receipts into the accounting records. A sub-ledger for individual member’s contributions is to be recorded for tax purposes.
- Maintain financial records of membership
- For a person to deduct a charitable donation on their personal tax Form 1040, charities as defined by the U.S. Tax Code 501(C)(3) are required to provide written statements. (United States, Internal Revenue Service). Thus, the organization must keep listings or sub-ledgers for individual member’s contributions. The written statements should be sent to the individual members on a six-month cycle with instructions regarding whom to contact concerning discrepancies in the organization’s financial records. A designated member of the Board should investigate any reported discrepancies to determine if it was an honest error or an irregularity, and then take the appropriate corrective action.

CASH DISTRIBUTION

Similar to cash receipts, there are a variety of cash disbursement schemes, as well as various corruption schemes. In comparison, two types of schemes, the distinction is where and when they occur during the procurement process. Corruption schemes attempt to influence the purchasing process. Thus, when cash is disbursed to pay an invoice, the payment appears legitimate and justifiable. Cash disbursement schemes misdirect funds in the payment process. Unlike cash receipt fraud, internal controls cannot be limited to one or two schemes. Therefore, the Board must implement a network of controls to provide adequate fraud deterrence.

The most common corruption schemes are kickbacks, bribery, bidding process fraud, and undisclosed conflicts of interest. Kickbacks are payments to staff members for approving payments to invoices for goods or services never delivered or with inflated pricing. Bribery occurs when staff members receive payments to influence the bidding process. The last corruption scheme occurs when staff members have a hidden economic or personal interest in the bidding process, which is adverse to the organization’s best interests.

Primary cash disbursement schemes are check tampering, billing and requesting reimbursements for personal expenses. Check tamper- ing schemes involve altering checks through forgery or changing the payee on written checks. Billing schemes are fraudulent payment on vendor’s invoices. These are accomplished by payments to vendors or fraudulent payment to legitimate vendors, which can include personal purchases and duplicate payments to vendors.

CONTROLS TO DETER FRAUD IN THE BIDDING PROCESS

Corruption schemes, like skimming, are difficult to detect. They occur before legal purchase contracts are formalized. The following steps aid in the deterrence of corruption schemes. First, the organization should have written ethics policies for the procurement process. Although this is a standard business practice, many religious groups view themselves as trustworthy, and view a written ethics policy as a personal affront. Second, the organization should have predefined procurement procedures with adherence to the competitive bidding process. Competitive bidding processes should include a formal Request for Proposal (RFP) that outlines the vendor’s performance and payment requirements, vendor qualification, requirements for multiple bids on each RFP, and final contract approvals by more than one person. The third step is to aggregate duties of the procurement functions. The functions of vendor approval, submittal of the RFP, purchase approval, and payment should be handled by more than one person. In addition, unused vendors should be rotated through each function to avoid establishing personal relationships with the vendor. The last step is to review the vendor’s work and audit the payments to the vendors. On a quarterly basis, a person outside the procurement process should review the vendor’s work to ensure it complex with the purchase agreements. The religious organization should ensure they received the quality goods or services contracted for and not substandard, unwanted, or non-negotiated goods or services. In addition, detailed reviews of the vendor’s procurement history should be conducted to detect any unusual pricing or pay- ments, which could indicate fraud.

- Controls to deter check tampering

There are two primary methods used in check-tampering schemes.

In the first method, the perpetrator uses blank checks to create personal payments. In the second method, the perpetrator redirect checks from vendors to themselves. Controls over blank checks and checks ready for mailing will deter most check-tampering schemes.

Religious organizations must start with control of blank checks. Most forgers will take the last check in a series of checks to create counterfeit checks. Therefore, the first step is to seal boxes of blank checks with security tape. Boxes with a broken seal are possible signs of stolen checks. The unused sealed boxes should be periodically checked for seals that have been tampered with or are broken. Next, the Treasurer should ensure checks are used in numerical sequence. This is especially important when a new box of checks is opened for use. Any non-sequential checks should be flagged for an audit of the check for check sequence numbers. Lastly, any voided checks should be recorded and the checks destroyed.

Organizations can control tampering by changing their check stocks and printing methods. It is easy and inexpensive for churches to use blank check stock which is a poor business practice. Religious organization should use high-quality check stock embedded with a distinct watermark. The paper color and watermark should be changed periodically. In addition, the font style used on the checks should be changed regularly to increase the difficulty of manufacturing counterfeit checks.

There are three methods to alter checks prior to delivery ranging from converting stolen checks to altering the checks payable. However, the key control for all checks is controlling the use of individuals. In a perfect environment, the people writing the checks would not be the ones entering the checks into the accounting records or mailing the remittance. However, in small religious organizations the people preparing the checks are usually the same people entering the disbursements into the accounting records. Thus, the organization must rely on compensating controls. The first compensating control is dual signatures (or one-over-one signatures) on all vendor check payments. When checks are presented for Board members’ signatures, the pay- ments should include the original checks, vendor remittance advice, the vendor invoices, and purchase orders. Two Board members should be required to sign the checks after reviewing and verifying the legitimacy of the payments. The checks are not returned to the bookkeeper but, should be mailed by a Board member. All signed
checks should be mailed immediately to avoid loss or tampering such as altering the check payees. Churches should consider zero-based budgets (ZBA) for vendor payments. A ZBA is a method to control disbursements. Money from the master accounts is transferred into the ZBA to cover the monthly checks. Thus, once all the checks are cashed by the vendors the account has a zero balance. Should a negative balance appear, it is possible an unauthorized check was issued and cashed.

• Controls to deter billing schemes

The primary control to eliminate billing schemes is a well-coordinated purchasing process. The basic step is to create a required specification for vendor performance, verification of a vendor, and a performance audit. Using cleaning services as an example, the Board should decide the level of services to be performed by the cleaning organization. Based on the specifications, a minimum of three vendors should be solicited to submit quotes. Visits should be made to each vendor’s office to ensure that the businesses actually exist and/or to the local library to research a database of local businesses to review the potential vendors’ histories. Once a vendor is chosen, a standing purchase order with terms and conditions should be signed. After the service is performed and the vendor submits an invoice, a check is prepared for the Board members to execute a one-over-one signature. The check should be accompanied by a signature package to include: a copy of the purchase order, confirmation of goods delivered or services performed, the invoice, and remittance advice. The package should be formed, the invoice, and remittance advice. This will ensure that payment is made to the work performed to ensure full contractual performance and sign the check. Once the policies are in place, the church should establish standard procedures for transactions within the accounting cycles. In addition, the policies should be reviewed and signed by two independent Board members prior to the actual reimbursement to the member claiming the expense. EXPENSE REPORTS

Expense reimbursement frauds occur when false or inflated expenses are listed as legitimate expenses on the expense report. There are four types of expense reimbursement schemes: reimbursed personal expenses, overstatement of expenses, fake expenses, and duplication of expenses. While there are a variety of schemes and many of these schemes can be difficult to discover, a few simple controls will allow the Board to deter the majority of reimbursement schemes.

The first step is to establish a reimbursement policy describing the types of expenses that are reimbursable, the maximum amount allowable for any expense type, and a period in which the expenses must be submitted for reimbursement. In addition, the policy should clearly and explicitly state that expenses will be reimbursed only with original receipts with no exceptions. Original receipts detailing the purchased items are important since unscrupulous staff members might attempt to submit photocopies, stubs, or even fake receipts for reimbursement. Once the policies are in place, the church should establish standard and detailed expense report forms to include original supporting documentation, dates and times of expenses, payment methods, descriptions, and the purpose of the expense. Expense reports must be reviewed and signed by two independent Board members prior to the actual reimbursement to the member claiming the expense.

CONCLUSION

The 360° Internal Control Model is designed to be a comprehensive control structure. It provides a full circle of accountability from all staff members and volunteers to the congregation. The internal control system reduces the fraudster’s opportunities by creating clear procedures for transaction, reporting, and internal controls. In addition, this proposed structure reduces the rationalization of the fraud by creating an accountability matrix. The accountability matrix has a two-fold effect with bond insurance and a fraud tip hotline. The bond insurance provides an external oversight and the tip hotline creates an internal oversight for the staff members and volunteers handling the financial affairs. Thus, this system completes the circle of accountability for any religious organization and those who put it into practice.

REFERENCES


ROBERT E. WILLEY, CPA, CFE, CGMA, holds a Bachelor of Science in History from Eastern Michigan University. He holds a Master of Science in Professional Accountancy from Walsh College of Accountancy and Business Administration. In addition, he recently received a Master of Science in Forensic Studies from Stevenson University. He currently works as a financial consultant to the National Cancer Institute.


The difficulty with reducing or eliminating terrorist financing is that terrorist organizations have a multitude of methods to obtain funding and continue to adopt their strategies as techniques are exposed. Terrorists use both formal and informal economic systems to fundraise and distribute money (Lormel, 4). Methods that utilize banking systems to transfer money between accounts as well as the use of credit cards are considered part of the formal economy (Lormel, 4). However, terrorists also utilize informal economic systems called the “hawala system” which allows them to move funds in a manner that is both “discrete and reliable” (Lormel, 11). The hawala system has been used for decades, as long as the Middle East has been at war, and Asian cultures, to move money around the world without having to set up foreign accounts (Brightman, 82). Aside from the traditional use, the hawala system is particularly attractive to terrorists as it leaves a minimal paper trail (Brightman, 285). It is a cash courier or trade-based service where brokers (hawaladars) operating in different countries communicate with one another to exchange cash or commodities without formally transferring money to each other (Samy, 7-8). 

Individuals approach a hawaladar to facilitate the movement of funds and with the exchange of a code the recipient receives payment (Samy, 8). Without funds actually transferred across a formal banking system and hawaladars retaining minimal accounting records, it is very difficult for law enforcement to trace transactions (Samy, 8). Traditionally used as a remittance service, terrorists and their supporters instead use the hawala system to share and distribute funds in a way that bypasses the regulations and surveillance of modern banking systems. By pursuing a comprehensive strategy to prevent identity theft in the formal economy, more resources can be dedicated to investigating the intricacies of the hawala system and other informal funding techniques. The transfer of money over the Internet has both expanded the capabilities of terrorists and complicated the prosecution process due to jurisdictional issues. Terrorists belong to Internet networks or forums known as “carders” who buy and sell credit card information obtained through hacking, phishing, and spamming (Pettit, 6). Terrorists do not necessarily have to be the ones stealing personal information but they work with carders who specialize in buying the information in bulk from hackers who sell for a profit (Pettit, 13). For example, in 2007 terrorists Younes Tousifi, Waseem Mughal, and Talir Al-Dousar united stolen credit card numbers obtained through phishing and Trojan horses to provide goods (equipment, airline tickets, cell phones) valued at $3.5 million to jihadis while also using the money to host terrorist organizations (Pettit, 17-18). Terrorists will continue to seek out new ways to obtain stolen personal information and credit card numbers through connecting with other criminals, especially in the financial sector, where they can fund their operations while remaining anonymous.

Utilizing fraud can help finance and facilitate terrorist plots as evidenced in the case of the “Millennium Bomber,” Ahmed Ressam. An Algerian-born terrorist living in Montreal, Canada, Ressam utilized several fraud schemes in his attempt to detonate explosives at the Los Angeles International Airport (LAX) during his Millennium celebration. In 1999 Ressam illegally entered Canada from France with a fake passport and worked with terrorist associates to plan a chemical explosion at the airport. He funded his plans by robbing tourists and selling stolen documents. Ressam obtained a Canadian passport under the name Benoit Norris by purchasing it from a document vendor and using a stolen blank birth certificate for supplementary proof. He then utilized the passport to travel to Afghanistan where he received al-Qaeda training and was requested to send back more Canadians to support his efforts to carry out the LAX plot. Ressam boarded a ferry to enter the United States through Washington state in a rented car containing explosives. Canadian and U.S. border agents initially did not suspect Ressam to be a terrorist as his pseudonym Benoit Norris was not included on their watch list. When border agents grew suspicious of Ressam’s behavior, they tried to escape but agents apprehended him and found explosives in the spare tire cavity of his vehicle (9/11 Commission Report, 177-179). Ressam cooperated with the FBI for two years providing them with information on al-Qaeda recruitment, training, and members (Ammirato, 1999, 2008). He was given a relatively light sentence of twenty-two years in federal prison with five years supervised release as a result of cooperating with the FBI, despite withdrawal of his testimony at a later time (Ammirato, Ahmed Ressam, 2002). The case of the Millennium Bomber indicates the irreducible complexity of a relatively unpoached plot that involved a small group of terrorists using copied documents and a fake identity that did not alert authorities. The case involved various U.S. and Canadian agents who successfully interrupted the plan and continued to seek more intelligence on terrorist networks and their operations.

PREVENTION AND DETECTION

Terrorists will continue to find areas of the U.S. economy and banking systems to exploit and it is the duty of individual citizens, businesses, law enforcement, and the state and federal government to take measures to secure personal information and to diminish terrorist financing. The responsibility of prevention must be appropriately divided in order to efficiently use resources, fund, and time while also minimizing potential losses.
The expansion of Joint Terrorist Task Forces (JTTFs) has been an essential component of the prevention and detection of terrorist activity. Now four times larger than its pre-9/11 size, JTTFs around the nation consist of, “small cells of highly trained, locally based, passion-ately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies” (“Protecting America”). The accomplishments of the JTTFs in identifying and preventing terrorist activity make the necessity of cooperation among today’s law enforcement officers. While the FBI and other law enforcement agencies identify identity thefts within complex financial schemes, their limited resources and heavy caseloads indicate that ancillary crimes such as identity theft must be more critically addressed by local law enforcement, the private sector, and individual citizens to adequately divide and share the responsibil-ity of prevention and detection.

The limited funding and resources available to federal and state law enforcement agencies illustrate the importance of partnerships between law enforcement and the private sector. The FBI’s InfraGard program has been successful at bringing the two together. InfraGard links professionals with local FBI field offices and provides an envi-ronment for dialogue regarding threats, alerts, and asset protection in addition to providing training sessions on cybersecurity and counterter-rorism (“About InfraGard”). Strengthening the exchange of information and ideas among policy makers, law enforcement, and the private sector will cultivate further cooperation and assistance to reduce the threat of terrorism.

PRIVATE SECTOR RESPONSIBILITIES

The private sector has a dual role in preventing identity theft and terrorist financing. It must actively protect private information while also developing new technologies and practices that will ensure information is shared and stored securely. Businesses facilitate trade as well as the movement of capital around the world, while acquiring a significant amount of information about individual citizens in the process. With terrorism an ongoing threat to business operations, it is important for the private sector to take steps to protect consumer and corporate information so that it is not used to propagate crime and terrorist activity.

Motivated by profit, minimizing losses, and customer satisfaction, the private sector will have to develop more effective ways of conduct-ing business security. In addition to reducing reputational risk, a proactive approach to personal information security will be lucrative for businesses in the long-term despite up-front costs. In addition to the point of sale businesses, the security of private information is critical to the financial and banking industries. Financial institutions have a legal responsibility to follow legal obligations to ensure customer information is accurate and suspicious transactions are reported. Guidance for specific customer identification programs and the reporting of suspicious activity are outlined in 1) the Bank Secrecy Act (transaction reporting standards); 2) the USA PATRIOT Act (anti-money laundering); and 3) the Gramm-Leach-Bliley Act (privacy standards). It is essential that the private sector, especially the finance and banking industries, understand the legal standards as well as set company policies that follow or exceed the minimum require-ments.

The private sector must also become better educated in the preven-tion of fraud, money laundering, and terrorist financing in order to actively participate in the detection and prevention of crime. To better assist law enforcement agencies and to more efficiently divide the work-load of detecting complex terrorist financing techniques, finan-cial intelligence units must be better staffed with trained personnel such as Certified Fraud Examiners and Certified Anti-Money Lau-ndering Specialists (“CTTF Working Group Report,” 7-10). A more knowledgeable private sector, well-versed in both the laws and the fraud schemes pertaining to terrorist financing, will enhance investi-gations, accelerate apprehension of criminals, and reduce time spent prosecuting offenders.

INDIVIDUAL CITIZENS’ EFFORTS

Individual citizens must play a larger role in preventing identity theft. With a better educated and more vigilant public, identity theft will become more difficult and individual citizens will become problem solvers rather than victims. A reduction of negligence in terms of pro-ecting personal information gives law enforcement and intelligence agencies more time and resources to focus on uncovering complex terrorist financing schemes, furthering their anti-fraud education, training others, and ultimately catching more terrorists. Individuals have a responsibility to protect their own information as well as hold-ing those they release their information to responsible for its security. Research shows that college students are particularly at risk for iden-tity theft based on the availability of their information on numer-ous databases (Hanel, 14). College students exchange information through social media websites, apply for jobs and loans that request personal information over the Internet, and receive electronic fre-quent mailings for credit card applications (Hanel, 14). “One out of five identity theft scams happens at a university or college, according to the Identity Theft Resource Center” (Hanel, 14). In addition to college students, children and the elderly are also frequent targets of identity theft (Hanel, 12). With identity thieves targeting vulnerable populations through the mail and on the Internet, it is essential that the public is aware of current scams and knows how to protect private data for themselves and others.

CONCLUSION

There is no single agency, person, or system that can defend against terrorism and identity theft. Previous instances of terrorists using fraud to conduct their activities have shown that when collective forces are not diligent or cooperative, the terrorists succeed. However, the instances of cooperation among the private and public sectors that have led to the arrests of terrorists and their co-conspirators are increasing. In July 2011, a chemical supplier, Carolina Biologi-cal Supply Co, and a freight company, Cross-Way Freight, separately reported the suspicious purchase and shipment of chemicals by Kha-lid Ali-M Aldawale, a twenty year old Saudi Arabian (Keller). The tipped led to the arrest of Aldawale by the FBI who searched his resi-dence and found evidence indicating that he was planning attacks on U.S. hydroelectric dams, nuclear power plants, and former President George W. Bush’s residence in Texas (U.S. Department of Justice). Aldawale wrote in his journal about using a forged U.S. birth certifi-cate and various driver licenses to carry out his explosive plots (U.S. Department of Justice). Without the information from the chemical and freight companies, the outcome of the situation could have been significantly worse.

Cooperation and awareness at all levels of society are indispensable factors when fighting terrorism and crime. Citizens cannot rely solely on the government and law enforcement agencies to ease the threat. Agencies must continue to foster community involvement and educa-tion to build valuable partnerships that promote working together to effectively reduce the likelihood of terrorism.

Targeting the source of money is an appropriate and feasible way to mitigate the threat of domestic and international terrorism. A reduc-tion in the occurrence of identity theft will make it more difficult for terrorists to obtain funding and to assimilate into American culture while developing new plots. Identity theft is an issue that every citizen can help prevent. Overall, the strategies implemented to reduce identity theft will have ongoing benefits as businesses will be able to focus on productivity and developing more secure ways of executing transactions, law enforcement agencies will devote more resources to complex and modern crime schemes, and governments and their agencies can work together to build stronger alliances to reduce ter-rorism around the world.

REFERENCES


Microstamping: The Last Frontier in Firearm Identification

Rocheh Benjamin

For the past one hundred years, law enforcement and expert forensic investigators have relied on various forms of firearm identification to assist in convicting gun crime suspects. Intentional Firearm Microstamping or microstamping is a breakthrough technology with the potential to dramatically alter the firearm identification landscape. Microstamping empowers police with the heretofore unattainable capacity to identify a firearm using only a single cartridge case.

This paper will explore the origins and implications of the microstamping method, how it compares with existing methods of firearm identification, and the feasibility of administering such a revolutionary firearm identification system. Additionally, this paper will weigh the benefits of microstamping against its costs, and determine whether it should be pursued in its current form, modified, or abandoned. Ultimately, this paper will argue that microstamping should be pursued in its current form with one caveat; more testing must be conducted to ensure its viability on a national scale.

Engineers Todd E. Lizotte and Orest Ohar of ID Dynamics, LLC invented microstamping in the 1990s to offer law enforcement a more effective means of providing both trace evidence in gun crimes and more information for targeting firearm trafficking. For over fourteen years they labored diligently in their Londonderry, New Hampshire laboratory to develop a method that would improve firearm identification and resolve the problems with existing methods. Rather than rely on the comparison of unintentional, incidental tool marks found on cartridge castings and firearms, Lizotte and Ohar explored a code system that could be intentionally stamped on each cartridge case when fired.

"This code would be instantly traceable, similar to a serial number, and provide police with an immediate identification of the firearm’s serial number, make, and model (Lizotte and Ohar, “Forensic,” 12). Furthermore, if the alphanumeric code can be partially recovered, even if the gear code fails as a backup, law enforcement still has more information than they would have had without microstamping. The legible digits provide some information on caliber, type, make or model (Lizotte and Ohar, “Forensic,” 14). Consequently, this information together with traditional firearm identification methods greatly reduces the number of possible firearm matches to that pinpointing the exact weapon is simpler.

Both the previous examples – an alphanumeric code being either completely or partially illegible – the gear code can still provide identification of a firearm’s serial number, make, and model (Lizotte and Ohar, “Forensic,” 2).

Lizotte and Ohar settled on an “optimized laser micromachining” process to engrave each firearm with two unique codes representing its serial number, make, and model, as seen in Figure 1. The primary or alphanumeric code is composed of a combination of eight letters and numbers, and is engraved on the firing pin tip, such that the digits are raised (Figure 2). When the gun is fired, the firing pin tip stamps the code on the center of the cartridge case primer. The primer is well suited to stamping because it is a softer metal than the firing pin tip.

The second code is the gear code. It employs unique geometric designs and is engraved on the round shaft of the firing pin. When the gun is fired, the gear code is stamped and used to stamp the gear code on the cartridge case when fired. This code can still provide identification of a firearm’s serial number, make, and model (Lizotte and Ohar, “Forensic,” 2).

FIGURE 1: Gear Code surrounding Alphanumeric Code

FIGURE 2: Firing pin tip with microstamp installed

Lizotte and Ohar, “Forensic,” 5)
face finish to ensure a clear, reliable code transfer. Since each firearm is engraved with a personalized code according to its performance through a process called optimization, these intentional marks repeatedly transfer successfully (Lizotte and Ohar, “Forensic,” 6).

The optimization process consists of a rigorous three-part test that occurs before a firearm is outfitted with a microstamping code. The optimization tests assess a firearm’s force of explosion, pressure, heat, gases, and any conditions that would affect the transfer process of the stamping technology (Lizotte and Ohar, “Forensic,” 6). The first test is the ‘cycle of fire analysis.’ In this test, shots are fired repeatedly and the used cartridge cases are analyzed to verify which surfaces of each cartridge case came into contact with the firearm, as well as each point of contact. These include the breech face, firing pin, ejector, magazine, and extractor. In this way, the tester can determine the best surfaces of the firearm for installing the microstamping technology. Next, a second group of test shots are fired and different ‘code resolutions’ are tried until the most effective character set is developed for the firearm. Finally, both the optimized character set and gear code are installed and a third round of test shots are fired to ensure that the stamp successfully transfers repeatedly (Lizotte and Ohar, “Extracting,” 7).

As a criminal activity and organized crime continue to spread, law enforcement faces the increasingly difficult task of tracing and identifying firearms. This has led state law enforcement agencies such as the Los Angeles Police Department to use database systems, i.e. Compstat, to help trace firearms by automatically analyzing and connecting evidence to create leads (Lizotte and Ohar, “Extracting,” 4-5). However, in order for these computer systems to be useful to law enforcement, a firearm must be recovered. Recovery tends to be a lengthy and often unsuccessful process thus giving criminals a tremendous advantage.

Another strategy for law enforcement has been the use of Geospatial Information Systems (GIS), a geographic computer system that stores, integrates, analyzes, and presents information on criminal activity according to jurisdiction or type via spatial ‘reference’ information. If GIS is used in conjunction with microstamping, it provides law enforcement more information on tracing firearms. Since the recovered cartridge casings provide these traces almost immediately upon retrieval, law enforcement will have the information necessary to keep track of crime patterns much closer to ‘real time’ when the crimes occurred (Lizotte and Ohar, “Extracting,” 6). This enables law enforcement to create more accurate crime patterns across all areas of crime so that they can target these critical areas.

Additionally, each time a microstamped cartridge case is recovered, it provides law enforcement with crucial pieces of information for mapping crime patterns. The code reveals the destination of a firearm (the crime scene from which the cartridge case was recovered) plus it leads to the firearm’s source, or where it was purchased (Lizotte and Ohar, “Extracting,” 6). Microstamping, law enforcement will develop a broader understanding of gun traffic patterns. Once both the starting point and ending point of each firearm used in a crime are established, law enforcement can identify travel patterns, conduct analyses, and determine where each firearm may now appear.

As a result, law enforcement is equipped with the necessary information to track gun traffic patterns and recognize hotspots for crime, faster, facilitating more efficient crime-fighting efforts (Lizotte and Ohar, “Forensic,” 3). Since each microstamped cartridge case recovered from a crime scene leads to a weapon, and each weapon leads to an owner or dealer, law enforcement can access important information on gun trafficking that would otherwise be unattainable.

Microstamping will also help deter straw purchasers, individuals who buy guns on behalf of others who are not legally permitted to purchase or own firearms. Straw purchasers will be more wary of purchasing illegal weapons since, with microstamping, there is a greater chance that a cartridge case used in a crime will be traced back to them (“Microstamping”). In order to protect themselves from being implicated in criminal activities, straw purchasers will avoid buying firearms both from and on behalf of unauthorized individuals.

In order for microstamping to be implemented, law must be passed requiring gun manufacturers to install the technology. In 2008, Congress passed the Technological Resource to Assist Criminal Enforcement, or TRACE Act, which proposed implementing microstamping, calling the technology “microstamping” or “microstamped” or “microstamping technology” (United States, House of Representatives, “Technological”). The bill seeks, “To require microstamping of all firearms manufactured in or imported into the U.S., and ballistics testing of all firearms in the custody of the Federal Government” (United States, House of Representatives, “Technological”). Although this bill was introduced by New Jersey Representative Robert Andrews in the 110th Congress, the bill was referred to the Committee on the Judiciary. To enforce the proposed microstamping requirement, Section 203 of the bill amends Title 18 of the United States Code by imposing microstamping requirements on firearms that fall under the manufacturer’s qualifications, will, after notice and hearing, have their firearm license revoked. The definition of a microstamped firearm according to the legislation is, “with respect to a firearm, that etched into the interior surface or internal working parts of the firearm is an array of characters which identify the make, model, and serial number of the firearm” (United States, House of Representatives, “Technological”). On July 1, 2010, H.R. 5667, the “Firearms Microstamping Evaluation and Study Act of 2010” was introduced before Congress (United States, House of Representatives, “Firearms”). If passed, this bill will mandate a comprehensive study on a national scale by the National Research Council of the National Academy of Sciences to determine the costs of implementing microstamping nationwide (United States, House of Representatives, “Firearms”).

Although microstamping has not yet been implemented at the federal level, California has enacted a microstamping mandate, and many states (Alabama, Arizona, Connecticut, Hawaii, Illinois, Indiana, Kentucky, Maryland, Mississippi, Missouri, New Jersey, New York, Pennsylvania, Rhode Island, South Carolina, Tennessee, and Washington) are considering following suit (Ammunition Accountability). In his article, “Microstamping Calls the Shots,” Douglas Page reports that in 45% of homicides in California there are no ammos made (Page, 1). The low arrest rate is a direct consequence of the ineffective methods for firearm identification currently in practice. As a result, on October 13, 2007, California Governor Arnold Schwarzenegger signed Bill No. 1471, the “Crime Gun Identification Act,” making California the first state to enact a microstamping law which went into effect in January 2010 (Page, 1).

The California Penal Code states that every semiautomatic pistol must be:

...Equipped with a microscopic array of characters that identify the make, model, and serial number of the pistol, etched or otherwise impressed in two or more places on the interior surface or internal working parts of the pistol, and that are transferred by impressing on each cartridge case when the firearm is fired, provided that the Department of Justice certifies that the technology used to create the imprint is available to more than one manufacturer unencumbered by any patent restrictions. (California Penal Code)

Although microstamping presents many advantages to gun crime investigation, its true benefit can only be understood when compared with traditional methods of firearm identification. Traditionally, firearm and tool mark identification have utilized ‘unintentional’ tool marks transferred onto ammunition as a result of the firing process. When a firearm is manufactured, the machining process creates nicks and scratches on internal surfaces of the firearm mechanisms. These tool marks are then transferred to the ammunition upon ejection (Lizotte and Ohar, “Forensic,” 5). Subsequently, when examined by firearm and tool mark identification experts, the marks found on ammunition can be matched to those found in the firearm and be used as evidence to identify the firearm used in the crime.

In his article, “Pattern Crimes: Firearms Trafficking Enforcement Techniques,” in the September 2008 FBI Law Enforcement Bulletin, Special Agent Joseph P. Gresko, who works for the Bureau of Alcohol, Tobacco, and Firearms (ATF) in Newark, New Jersey, describes the process of tracing a firearm, without the aid of microstamping. First, a firearm must be identified as the source of a cartridge case found at a crime scene. The next step is tracing the firearm. This is done by locating the ATF Firearms Transaction Record, a form the firearm purchaser must fill out at the time of the transaction. The dealer must retain the form for as long as he remains in the business of selling firearms (Gresko, 6). That way, if the firearm is involved in a crime, it can easily be traced back to the purchaser.

The dilemma is that although an ATF Firearms Transaction Record can lead law enforcement to the purchaser of a specific firearm, that can only happen after the cartridge case found at the crime scene is matched to the firearm. In order to make the comparison, both the cartridge case and the firearm must be recovered. This severely handicaps firearm tracing because over fifty percent of the time the firearm used in a gun crime is not recovered. In those instances, the information retrieved from the recovered ammunition is stored in a database for future comparison but does not provide any immediate identification (Lizotte and Ohar, “Forensic,” 5).

Microstamping will save both time and effort for forensic investigators in the firearm identification process. As long as a single cartridge case is retrieved from a crime scene, the code stamped onto the cartridge case will provide an important lead. Since the code identifies the weapon used in the crime by serial number, make, and model, even if the actual weapon is not recovered, law enforcement is aware of the exact weapon used in the crime. Then, through the ATF Firearms Transaction Record, law enforcement should be able to track down the dealer who sold the weapon originally as well as the person who purchased it (Lizotte and Ohar, “Extracting,” 2). Consequently, if the owner or dealer was involved in the crime, the microstamp will have led law enforcement to two viable suspects or two valuable sources of information.

The presumably unique tool marks used in firearm identification are known as a firearm’s fingerprint. Matching the fingerprint on a cartridge case to that of a firearm is known as ballistic fingerprinting. The analysis of the fingerprinting is performed by expert firearm and tool mark examiners who either study the marks manually (traditional examination) or with the aid of computerized database systems via ballistic imaging (National Shooting Sports Foundation).

The process of ballistic imaging utilizes the “cycle of fire analysis” in which test shots are fired from a recovered weapon to compare the tool marks on the test cartridge casings with those found on a cartridge case recovered from a crime scene. The test results are then stored in a database for future reference (National Shooting Sports Foundation).

While these current methods of firearms identification have proven useful to some extent, their success is hindered by many issues. First, taxpayers are concerned of the vast dollars being spent on ballistic imaging, especially since it does not significantly help solve crime. This concern is setting in motion a movement to abolish the use of ballistic imaging entirely (National Shooting Sports Foundation, “Ballistics”). Second, because positive firearm identification...
ion requires the recovery of both a cartridge case and a firearm, and more often than not a firearm is never found, the ballistic cartridge images are stored in a national computer network, the National Integrated Ballistic Information Network (NIBIN), to which numerous law enforcement groups throughout the United States contribute (National Shooting Sports Foundation). Consequently, mass amounts of information stored on the database force reviewers to sort through a vast amount of images to compare tool marks to match a firearm to a cartridge.

Furthermore, it can be years before a weapon is recovered, if at all. Upon recovery and in order for a positive identification to be made, test shots must be compared with crime scene cartridge casings stored on the database. This lengthy process and elapsed time reduces the overall effectiveness of ballistic fingerprinting.

Additionally, while the National Integrated Ballistic Information Network stores digital ballistic images and compares those to find matches that can link multiple crimes to a single firearm, the network only matches an image to those that are the most similar. Firearm examiners must microscopically review the possible matches against the firearm case found at the crime scene to determine if the cartridge truly matched (United States Department of Justice). Although the network contributes to tracing firearms, it still requires manual labor and time on the part of firearms examiners.

Contrarily, microstamping allows the identification of a firearm the first time it is used without needing to recover the firearm itself. Lizotte notes that this is the shortest time-to-crime identification process possible with any firearm technology (Lizotte and Ohar, "Forensic," 7-8). As Lizotte and Ohar explain, when humans, who are expertly trained in firearm identification, are replaced with automated identification technology, the time and labor on the part of firearms examiners is replaced with a more efficient system to recover and match the firearm.

A recurring problem in firearm identification is multiple striking. Normally, when a trigger is pulled, the firing pin strikes the cartridge case causing it to be ejected from the chamber. However, sometimes a single pull of the trigger causes the firing pin to strike the cartridge case multiple times resulting in a smudged printing much like the one seen in Figure 3. Although researchers have expressed concern about the effect of a multiple strike on a microstamp transfer, Lizotte explains that these same concerns apply to traditional examination and ballistic imaging (Lizotte and Ohar, "Forensic," 7-8). In fact, current ballistic fingerprinting methods never analyzed multiple strikes in firearms or ammunition, so the number of times a firing pin could strike was unknown until microstamping was tested (Lizotte and Ohar, "Extracting," 14). Tests conducted on a 1911 Automatic Caliber Pistol (ACP) confirmed that double strikes occur 73% of the time, and a firing pin could strike five times per a single pull of the trigger (Lizotte and Ohar, "Extracting," 14). The 1911 ACP which was first made by John Browning in 1911 has been remodeled several times in the past decades and is still a popular model used today by civilian gun owners, the military, and law enforcement (Caradina).

While microstamping improves upon many ballistic fingerprinting deficiencies, researchers question its reliability, its thoroughness in addressing possible risks, and its effect on crime. A University of California – Davis study of microstamping, largely researched by forensics student Michael Beddow, concluded that microstamping is “feasible, but flawed,” since the technology only worked with some types of firearms and ammunition, indicating that more testing is necessary to ascertain the cost of the technology and whether or not it should be implemented on a state level (Page, 1).

As part of the study, a variety of firearm models with varying characteristics were tested using different types of ammunition, including five semi-automatic pistols, two semi-automatic rifles, and one shotgun. The firearms used were all readily available on the street and among the most commonly used by criminals (Howitt, Tulleners, and Beddow, 20). Each was laser-engraved with a microstamp on its firing pin. Based on the test results, which demonstrated that the technology worked well on some firearms and ammunition combinations, while on others transferability was weak, Beddow concluded that while the technology has potential, there remain several areas that need to be further researched before the technology should be required by law (Howitt, Tulleners, and Beddow, 12-14). These areas include several sets of experimental conditions selected from best practices, a study of ammunition types, and further research on the technology's effectiveness with different types of ammunition and found that the alphanumeric code and gear code were examined, and in nearly every case the gear code was able to provide the entire alphanumeric code. The study concluded that while using optical microscopy, a lower level resolution, the code was retrieved over 90% of the time (Lizotte and Ohar, "Forensic," 10-14), which means that a higher level resolution would have an even greater transfer rate. In conclusion, the technology improves on the current firearm’s ability to transfer stamps reliably to ammunition and will thus be of great assistance to law enforcement tracing efforts.

Based on the results from studies done, the technology is both reliable and successful. According to a 2000 study by the Bureau of Alcohol, Tobacco, Firearms, and Explosives, semi-automatic handguns have an average time-to-crimetime of 1.6 to 6.4 years and do not fire for more than 500 rounds by the time the weapons are used in crime (Page, 2). This means that by the time a firearm is used in a crime, the microstamping will still transfer successfully based on the NanoTag™ tests cited above with success after 2500 rounds.

Another drawback to microstamping has been argued by the National Shooting Sports Foundation. Douglas Page acknowledges this in his article and writes that the microstamping bill fails to realize its effect on the black market (Page, 2). If the microstamping law is passed, then criminals are more likely to use microstamped firearms because of the trouble that microstamped cartridge cases by illegally trafficking in non-microstamped firearms with the potential to create a new black market.
Further, there are numerous firearms already in circulation that cannot be microstamped. These guns will limit the capacity for microstamping to successfully change the law of weapon identification and firearm identification. Criminals will choose to acquire non-microstamped firearms because they limit the choice of microstamping as a tool to help law enforcement solve gun crimes.

One might argue that although issues of chain-of-custody exist and can limit microstamping as a tool to provide evidence in court, these same issues exist in current methods of firearm identification. Using ballistic imaging or traditional examination to investigate a gun crime does not eliminate problems of stolen firearms or planted evidence (Murdadyn, 10). Instead of pointing out such flaws, as unique to microstamping, whose goal is to provide leads in gun crimes, and not necessarily evidence to be introduced in court, these questions should be asked of firearm identification in general. Preventing microstamping from implementation when firearm identification is nationally accepted despite these same flaws appears illogical.

Another way criminals circumvent the technology is by intentionally removing it so that the stamp cannot transfer legibly. As Page advises, the microstamping engraving on the firing pin is no more than one-thousandths of a millimeter deep and can easily be rubbed off with household tools (Page, 2). George G. Krivosta, a firearms expert of the Suffolk County Crime Laboratory in Hauppauge, New York, proves this point in his article “NanoTagTM Markings from Another Perspective.” Krivosta writes about an individual who, while testing the stamp’s durability, removed the stamp completely, in minutes, using only a sharpening stone that was lying around his house (Krivosta, 43).

Nevertheless, as Lizotte points out, this is a fault of any form of firearm identification (Lizotte and Ohar, “Forensic,” 9). Just as someone can scrape away at a fingerprint and render it unreadable, a criminal can scrape away at traditional marks and alter their appearance, or remove them completely, making comparison of the tool marks nearly impossible.

Moreover, as the UC-Davis study mentions, defacing a microstamping engraving on the firing pin would require the firing pin to be removed from the firearm (Fischer, 40). However, Baltimore Commissioner Frederick Bedford explains that the majority of people [in Baltimore] do not know how to “gunsmith” (Fischer, 39). “People hardly know how to operate their guns safely, let alone take them apart and ‘file off’ the engraving on the firing pin (Fischer, 39).”

As Lizotte explains, it is not uncommon for a criminal to alter a firearm by sawing off the burr of a chamber, or replacing it with a different size barrel. This changes the caliber of a weapon completely making positive firearm identification extremely difficult with traditional comparison or ballistic imaging. Both of these methods rely heavily on linking a cartridge case to a firearm by caliber (Lizotte and Ohar, “Forensic,” 8). With microstamping, an altered firearm can still be traced through the code because no matter what caliber a firearm becomes, and what ammunition is used, the stamp remains the same.

Another drawback to microstamping is its cost. For gun owners, who need to constantly replace firing pins, the added cost of installing the microstamping technology can be burdensome. It can also become a large expense for law enforcement and the military because all firearms are manufactured in the same plants at the same time (Page, 3). So, even if only some states require microstamping, since firearm plants are located throughout the country, it will affect legal gun users and owners nationwide, unless there are specialized plants built for the states requiring microstamping.

In response to the concern over the cost of microstamping, NanoTagTM promises that the cost will not be more than eight dollars per firing pin in the first year of the technology’s implementation, and then the cost will go down to approximately two dollars in the following years (Page, 3). Therefore, microstamping will not become a significant financial burden to manufacturers, the government, or gun owners.

As a firearm identification expert, Krivosta questions NanoTagTM’s suggestions to install the technology on additional firearm surfaces such as the breech face, ejector, and inner chamber, for preventing illegal transfers as a result of either intentional or unintentional defacement. Without further testing, these surfaces are not practical for many reasons:

1. Head stamps on cartridge casings could ‘interfere’ with the stamp;
2. Where the breech face comes into contact with the cartridge case there is less pressure and the brass is harder so it does not get stamped easily, even with traditional marks;
3. The primer is softer so the stamp is transferred easily, but other parts are harder and won’t be impressed as well;
4. In some semi-automatic pistols with recoil, the cartridge case will shift and bruise hard against the breech face and transfer the impressed information from the stamp;
5. In guns operated semiautomatically, which have bolts that lock by rotating, the stamp could get ruined as well;
6. Marks on the breech face and ejector could also be defaced intentionally;
7. The surfaces shown by NanoTagTM to have stamps, the ejector and extractor, do not even come into contact with the cartridge case;
8. If the stamp was placed in the chamber, it would have to be far enough inside where the cartridge case comes into contact with it. However, the marks would also be easily ruined during extraction when the case moves (Krivosta, 44-46).

While the reasons listed above are valid, and more testing is necessary of microstamping, it is to be installed on additional firearm surfaces, the firearm surfaces being suggested for microstamping have been tested and yielded positive results.

In weighing the costs and benefits of microstamping, it is crucial to keep the goal of microstamping in sharp focus. Its goal is not to improve upon firearm mechanisms, as both researchers Krivosta and Beldow imply through their criticisms of the technology. If that were the case, it would be imperative that the technology be improved, so as not to cause unfortunate accidents. But microstamping is not meant to be a part of the firearms. Rather, as Lizotte and Ohar explain, the purpose is to improve upon current methods of firearm identification and illegal gun crime (Lizotte and Ohar, “Extracting,” 9). As Lizotte elucidates, “Since microstamping is a forensic tool, the criterion for success [is] being able to extract the code from the mark produced (Lizotte and Ohar, ‘Forensic,’ 12).” Based on initial positive test results, it appears that microstamping will accomplish this goal.

However, microstamping requires retooling for the entire firearm industry, yet will not help in every case. Therefore, before microstamping is implemented on a national level, more thorough testing must be conducted to evaluate microstamping’s viability across the entire range of firearms available in the U.S., to identify the precise costs for the government, manufacturers, and firearm owners, and to analyze those costs against the benefits of the technology.

The advent of every new technology is accompanied by critics, proponents, and adverse to change. Microstamping has added to this dialogue. If microstamping is disadvantageous, it can be discontinued. The initial studies of microstamping promise that failure to continue pursuing and refining this technology could be a loss to the firearm identification community.

REFERENCES


A Sticky Wicket: Transferring Protected Data from the European Union to Comply with the Foreign Corrupt Practices Act Without Violating European Privacy Laws

Kathy Kirkish, CFE

INTRODUCTION


United States House of Representatives. "Microstamped Firearms Deliver Data for Illegal Firearm Traffic Extraction Ballistic Forensic Intel-

The competing interests of the FCPA and European privacy laws create a predicament for American multinational companies that must transfer protected data from its European operations to its corporate headquarters in order to investigate and report FCPA violations. It may become a compliance nightmare when the data is stored in electronic form on virtual servers throughout the globe. One method by which American multinational companies can satisfy the opposing requirements of these laws is through the U.S.-European Union Safe Harbor Framework Privacy Principals Certification Program. To avoid prosecution and penalties imposed for violating a myriad of U.S. and foreign laws, it will require a team of professionals to solve complex legal, technical, accounting and forensic issues when conducting investigations on foreign soil.

THE FCPA

On March 30, 2011, Robert Mueller, the Director of the Federal Bureau of Investigation (FBI) informed the Senate Judiciary Committee that in 2010 the aggressive efforts of the FBI and the Department of Justice resulted in the recovery of over 1 billion dollars in fines for violations of the FCPA (United States, House Judiciary Subcommittee, 10). Hefty fines, as well as civil and criminal prosecution of American multinational companies, its officers, employees and agents, as a result of the FCPA violations, caught the attention of corporate America. The FCPA states it is a crime, not only to pay a bribe to a foreign official in order to obtain a business advantage, but also to fail to properly document such payments in the company's financial records. Generally, the FCPA applies "to any individual, firm, officer, director, employee or agent of a firm and any stockholder acting on behalf of a firm" (United States Department of Justice). U.S. corporations and foreign corporations that have issued and registered stock with the Securities and Exchange Commission (SEC) (known as "Issuers") or those entities required to file reports with the SEC are subject to the FCPA (Queler, Wu, and Chin [Sec 27.2]). According to the Department of Justice, a "citizen, national or resident of the United States" including sole proprietorships or U.S. legal entities formed to conduct business (known as "Domestic Concerns") are also subject to FCPA enforcement. Both Issuers and Domestic Concerns can be prosecuted for violating the FCPA when acts that occur either within the United States or outside of the United States result in payment of bribes to, "a foreign official, a foreign political party or party official, or any candidate for foreign political office" (United States Department of Justice). American multinational companies and citizens who facilitate or acquiesce to the payment of bribes by subsidiary operations to foreign officials can be found guilty of violating the FCPA. In 1998 the FCPA was amended allowing enforcement against foreign companies or foreign persons who participate in acts promoting the payment of bribes on American soil (United States Department of Justice).

ACCOUNTING REQUIREMENTS

The Securities and Exchange Commission (SEC) oversees a corporation's compliance with the accounting provisions of the FCPA. The FCPA requires corporations that have issued securities registered in the United States or corporations required to file periodic reports with the SEC to establish record keeping procedures that comply with General Accepted Accounting Principles (GAAP). Accurate books and records that insures the protection and truthful reporting of the company's assets are to be maintained. The company must retain external auditors to audit its books and records (Samangelo, Stein, and Jacobs, 36). They must also implement systems, "capable of detecting and preventing improper payments to foreign officials" (Queler, Wu, and Chin [Sec 27.1]). It is not necessary for the SEC to prove intent, i.e. that an illegal payment was made to procure an unfair business advantage. The mere failure to report a payment on the company's books or falsely report the purpose of a payment can subject the company to penalties and prosecution under the FCPA. The failure to establish a proper "system of internal accounting controls" as well as the, "conscious disregard" of accounting requirements can subject a company to criminal prosecution (Queler, Wu, and Chin [Sec 27.2]).

The increase in FCPA enforcement actions in the past few years is the result of American multinational companies' self-reporting efforts. The Department of Justice has encouraged companies to report confirmed instances of FCPA violations with the promise that self-reporting will lessen penalties assessed against the company. However, there is a condition for qualifying for a lighter penalty. The company must demonstrate it had established and maintained an effective FCPA compliance program to qualify for leniency (Samangelo, Stein, and Jacobs, 32-33).
COMPLEX CROSS-BORDER INVESTIGATIONS

Conducting internal investigations of corruption and bribery on foreign soil is a very different undertaking. FCPA violations may have occurred over a period of years involving employees, agents hired by American multinational corporation, and third parties. The volume of information that must be collected and examined is enormous. Relevant data may be found in several locations and in a variety of formats. To conduct thorough internal investigations, data must be collected from all locations if “...even remotely related to the matter at hand.” (Biegelman and Biegelman, 297)

Document relevance relevant to an FCPA investigation can involve a plethora of financial reports, business operations, and corporate maintenance records. It may be necessary to collect and analyze personnel files, as well as e-mail communications and attachments. Most corporate business information is stored and filed in electronic or digital format. To reduce costs, many corporations utilize third parties, such as cloud-computing services, to store and process business data. Cloud computing services host the company’s data on virtual servers located on continents other than where the subsidiary operation is located (Manning, 19).

The gathering of data pertinent to suspected FCPA violations include the preservation of the electronic document’s underlying or meta data. The preservation of electronic data is paramount, particularly if commercial litigation is expected, or an investigation by the Department of Justice, the SEC, or the IRS. When there is a question that an issue or incident may lead to commercial litigation, American multinational corporations are bound under the Federal Rules of Procedure 37(a) to preserve relevant electronic data.

EUROPEAN UNION’S PROTECTION OF ITS CITIZEN’S PERSONAL DATA

Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 was enacted in 1998 to protect the privacy rights of its citizens as it pertains to, the “processing of personal data and the free movement of such data” (Directive 95/46/EC, 1). The European Union was created in 1993 as a result of the Maastricht Treaty. Twenty-seven member countries of the European Union, benefit not only from a common currency, but also from the recognition and protection of individual privacy, human rights and human dignity (Bennett). A German labor court found that Walmart’s corporate code of ethics may violate German’s privacy laws, because it requires employees to report suspected violations of the corporate code of ethics (Bennett).

The DANGERS OF CLOUD COMPUTING

American multinational companies face another challenge in complying with European privacy laws when their European subsidiary operations contract with third parties for information technology and cloud computing services. With companies seeking to streamline business operations and cut costs, the use of virtual servers to store data and software applications offered by cloud computing services has dramatically increased in the last few years. Companies can similarly subcontract to third-party technology services, a cloud computer service provider, when these service providers allow users to access data at any time from any device.

The stringent protection of the personal data of European Union citizens stands in stark contrast to U.S. laws which provide weak protection of U.S. employees’ work privacy rights. In contrast, with the Member countries of the European Union, it has become common practice for companies to subcontract their technology services, e-mail and voicemail communications stored, or transmitted via internal communication systems. The “providers exception” of the Federal Communications Act permits an employer to access the content of an employee’s electronically stored information “as it is fit” without violating employees’ privacy rights (Starr and Warren, 136). Companies can also monitor employees’ phone calls for legitimate business purposes pursuant to the “ordinary course of business exception” of the Electronic Communications Privacy Act of 1986 (“ECPA”) (Starr and Warren, 134). Employees’ internet access, instant messaging and website postings may also be monitored (Starr and Warren, 137).

When the European Union data subject gives explicit consent for the collection and processing of his personal data, the company must disclose to the data subject the identity of the entity for which it is collecting the data, the purpose for the data collection, and the identity of the data recipients. The company must also provide the data subject an opportunity to correct data it collects and reports about the data subject (Directive 95/46/EC: Article 10 (a), (b), (c)). It must guarantee the data subject the opportunity to obtain the collected data, “without cost, at reasonable intervals and without excessive delay or expense...” (Directive 95/46/EC: Article 12). The company must also correct inaccurate information reported to third parties about the data subject (Directive 95/46/EC: Article 12).

The U.S. Sarbanes Oxley Act was created in an effort to eradicate financial statement fraud by publically traded corporations. The reporting requirements of U.S. companies under the Sarbanes Oxley Act of July 30, 2002, conflict with Directive 95/46/EC. The Sarbanes Oxley Act requires companies to establish a code of ethics and implement methods which permit the anonymous reporting by employees of questionable “financial improprieties.” This has resulted in the implementation of telephone hotlines or fraud hotlines by U.S. companies for the reporting of suspected incidents of fraud. The implementation of hotlines by American multinational companies at European subsidiary operations conflicts with the Directive and the separate privacy laws enacted by Member Countries (Bennett). For example, France determined that hotlines violated, “French principles of individual privacy, human rights and human dignity” (Bennett). A German labor court found that Walmart’s corporate code of ethics may violate German’s privacy laws, because it requires employees to report suspected violations of the corporate code of ethics (Bennett).

WHAT IS PERSONAL DATA?

The Directive defines personal data as, “any information that will identify a natural person by identification number, or physical, physiological, mental, economic, cultural and social identifiers and sexual orientation” (Directive 95/46/EC: Article 2(a)). This data includes the subject’s names, phone numbers and even addresses listed in telephone books (O’Brien). The processing of personal data is generally handled by information, which involves the use of the personal data, its automatic retrieval, disclosure or transmission, as well as the blocking, dissemination or destruction of the personal data (Directive 95/46/EC: Article 26(b)).

If the cloud computing services use “server virtualization,” the collected confidential data may be stored in “containers” on the same server along with another company’s data (Manning, 20). Although, there may be no threat to the data, a study performed by the National Computing Centre found that cloud computing services can experience system crashes, data loss, data corruption, and data theft (Armstrong, Barnett, and Davis). Therefore, it is imperative that American multinational companies enter into binding data protection agreements with cloud computing services whose security measures meet the stringent standards of the Directive and the Member country’s own privacy laws.

THE U.S.-EUROPEAN UNION SAFE HARBOR FRAMEWORK

To facilitate trade between Europe and the United States, the European Commission and the U.S. Department of Commerce’s International Trade Administration negotiated an arrangement, agreeable to both, for the acceptable flow of protected data from the European Union to the United States. The result was the U.S. European Union Safe Harbor Framework. The principles stated in the Safe Harbor Framework reflect a compromise of U.S. privacy standards and the European Commission’s requirements for the adequate protection of personal data (United States Department of Commerce, Introduction).


The Safe Harbor Framework is a process by which qualified American multinational companies voluntarily “self-certify” to the Department of Commerce that they have developed, implemented, and complied with privacy principles thus ensuring adequate protection of protected data

The Directive requires companies to, “implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, unauthorized disclosure or access, in particular when the processing involves the transmission of data over a network, and against all other unlawful forms of processing” (Directive: Article 17(1)). American multinational companies abridge their control function when they opt to use cloud computing services, outsourced suppliers, and third party providers.

In the event that a cloud computing service uses “server virtualization,” the collected confidential data may be stored in “containers” on the same server along with another company’s data (Manning, 20). Although, there may be no threat to the data, a study performed by the National Computing Centre found that cloud computing services can experience system crashes, data loss, data corruption, and data theft (Armstrong, Barnett, and Davis). Therefore, it is imperative that American multinational companies enter into binding data protection agreements with cloud computing services whose security measures meet the stringent standards of the Directive and the Member country’s own privacy laws.


The Safe Harbor Framework is a process by which qualified American multinational companies voluntarily “self-certify” to the Department of Commerce that they have developed, implemented, and complied with privacy principles thus ensuring adequate protection of protected
data. Companies participate in the Safe Harbor Program by providing the Department of Commerce a letter, signed by a corporate officer, which certifies that the company meets the standards of the Safe Harbor Framework (United States Department of Commerce, Self-Certification).

CONCLUSION

As more American corporations enter the global business market it will be necessary for these companies to monitor their conduct on foreign soil, ensure compliance with foreign regulations, and handle data appropriately. It will take a team of sophisticated professionals, including attorneys, IT specialists, Certified Public Accountants, Certified Fraud Examiners, Human Resource Professionals and forensic experts to successfully navigate this compliance minefield.

REFERENCES


Brooke Bivenk

FORENSICS JOURNAL

FALLIBILITY ISSUES IN FORENSIC EVIDENCE

KATHY KIRKISH is a Certified Fraud Examiner. As an employee of a federal contractor, she works in Homeland Security Investigations performing financial investigations of drug trade organizations, money laundering schemes, bulk cash smuggling, and intellectual property rights violations. Ms. Kirkish locates assets acquired with criminal proceeds for asset forfeiture purposes. In the past, she conducted civil investigations of financial crimes on behalf of law firms and fidelity carriers.

In 1976, Fred Zain started working for the West Virginia Department of Health and Human Resources. He was a member of a biology unit (a lab testing budly fluids) where he tested materials from crime scenes to detect any serums that could be used to identify possible suspects and aid police and prosecutors in obtaining convictions. Prosecutors quickly identified him as a valuable witness whom they could persuade jurys of the certainty offered in his lab findings. He would speak from a position of unimpeachable authority even if his colleagues disputed with him, which was often (Daff, p. 1). Zain was able to find traces of blood, semen or saliva that other technicians missed; he ran tests and crafted reports expertly supporting his conclusions, helping to garner guilty verdicts on cases with little or no other evidence. Always wearing a full police uniform at work and in court, Zain proved to be a formidable asset during hundreds of trials where he appeared as the expert witness on behalf of the state. When he testified, the prosecution often won the case (Kurland, p. 275).

Glen Dale Woodall would mean the beginning of the end for Fred Zain. Woodall, 25, was a gravedigger who worked at a cemetery across the street from a shopping mall where two women were raped in the winter of 1987. Because the rapist’s face was masked, neither woman was able to identify her attacker during the police investigation. Zain seemed to have an affinity for these types of cases as it allowed him to provide the critical piece of evidence that unequivocally implicated the suspect when other evidence could not. Zain testified that semen samples recovered from the victims were consistent with Woodall, who was found guilty and sentenced to life in prison (Fish, p. 236). In 1992, DNA testing cleared Woodall of any guilt and further proved that the initial tests done by Zain actually excluded Woodall as a possible suspect (Kurland, p. 275). Woodall sued the State of West Virginia for false imprisonment and received a $1 million settlement after spending five years in prison (Cleveenger). Ten men have since been exonerated in West Virginia upon discovery of Fred Zain’s appalling tactics (National Research Council, p. 44).

Fred Zain is often referred to as the rogue forensic scientist who undermines the credibility of otherwise critical, hard working forensic professionals everywhere who are dedicated to uncovering the facts in service of the criminal justice process. Zain’s corrupt legacy forces a reexamination of the criminal justice system’s identification of patterns denoting fraud and error by experts, and the limitations of DNA technology.

In 2009, Brandon L. Garrett and Peter Neufeld, co-director and co-founder of the non-profit legal clinic known as The Innocence Project, conducted a review of trial transcripts from 137 wrongful conviction exonerations where forensic analysts provided testimony during trial. The review indicated 82 cases (68%) involved invalid forensic science that offered conclusions, “mistraining empirical data or wholly unpoptort by empirical data” (Garrett). The findings of this study are troubling and necessary further exploration regarding the role of forensic fraud and error. Looking forward, the value associated with forensic testimony will only increase as technology becomes more exacting and precise; however, the incidences of fraud and error could irreversibly damage the credibility of many forensic disciplines, rendering them obsolete with the possible exception of DNA-based tests. This paper seeks to define and explore the elements, techniques and frequency of forensic errors and fraud, as well as examine the potential impact on the criminal justice system. Additionally, specific reforms proposed by individuals, organizations and the forensic community to mitigate forensic fraud and error will be considered.

ERRORS

What is a forensic error? For the purposes of this report, forensic errors include unintentional mistakes caused by human operators i.e. not the result of criminal or malicious intent. Five common activities prone to errors include: 1) death investigation determinations; 2) collection, handling, and storage of evidence; 3) sampling mislabeling of evidence; 4) sample contamination; and 5) operator bias. Death investigations can provide the critical foundation for a criminal investigation by revealing detailed information about the cause, timing and manner of death. Determining role of forensic fraud and error. Looking forward, the value associated with forensic testimony will only increase as technology becomes more exacting and precise; however, the incidences of fraud and error could irreversibly damage the credibility of many forensic disciplines, rendering them obsolete with the possible exception of DNA-based tests. This paper seeks to define and explore the elements, techniques and frequency of forensic errors and fraud, as well as examine the potential impact on the criminal justice system. Additionally, specific reforms proposed by individuals, organizations and the forensic community to mitigate forensic fraud and error will be considered.

ERRORS

What is a forensic error? For the purposes of this report, forensic errors include unintentional mistakes caused by human operators i.e. not the result of criminal or malicious intent. Five common activities prone to errors include: 1) death investigation determinations; 2) collection, handling, and storage of evidence; 3) sampling mislabeling of evidence; 4) sample contamination; and 5) operator bias. Death investigations can provide the critical foundation for a criminal investigation by revealing detailed information about the cause, timing and manner of death. Determining role of forensic fraud and error. Looking forward, the value associated with forensic testimony will only increase as technology becomes more exacting and precise; however, the incidences of fraud and error could irreversibly damage the credibility of many forensic disciplines, rendering them obsolete with the possible exception of DNA-based tests. This paper seeks to define and explore the elements, techniques and frequency of forensic errors and fraud, as well as examine the potential impact on the criminal justice system. Additionally, specific reforms proposed by individuals, organizations and the forensic community to mitigate forensic fraud and error will be considered.

ERRORS

What is a forensic error? For the purposes of this report, forensic errors include unintentional mistakes caused by human operators i.e. not the result of criminal or malicious intent. Five common activities prone to errors include: 1) death investigation determinations; 2) collection, handling, and storage of evidence; 3) sampling mislabeling of evidence; 4) sample contamination; and 5) operator bias. Death investigations can provide the critical foundation for a criminal investigation by revealing detailed information about the cause, timing and manner of death. Determining role of forensic fraud and error. Looking forward, the value associated with forensic testimony will only increase as technology becomes more exacting and precise; however, the incidences of fraud and error could irreversibly damage the credibility of many forensic disciplines, rendering them obsolete with the possible exception of DNA-based tests. This paper seeks to define and explore the elements, techniques and frequency of forensic errors and fraud, as well as examine the potential impact on the criminal justice system. Additionally, specific reforms proposed by individuals, organizations and the forensic community to mitigate forensic fraud and error will be considered.
and is regarded as a cautionary tale for employing proper techniques and following procedure when documenting a crime. According to William C. Thompson, a member of Simpson’s defense team, the “not guilty” verdict rendered by the jury was “not about the science, it was about the documentation.”

Forensic fraud is a complex concept to define as it requires proof of malicious intent on the part of the forensic professional. Negligence, incompetence, misconduct and outright bias are all points on a spectrum of malicious intent that is presented to a jury during the closing argument of a trial and by mischaracterizing such testimony the prosecution or defense increases the likelihood that a jury will begin deliberating before all evidence is understood and accepted allowing for more accurate analysis through the application of probability statistics.

The final type of forensic fraud is bias. Knowledgeably providing false or misleading testimony is perjury. Although the definition is simple, the act can range from blatant to subtle. This type of fraud involves law enforcement and/or forensic science personnel providing sworn testimony, documents or reports intended for the court that contain known deceptive or misleading information, findings, opinions or conclusions offered to secure unfair or unlawful advantage (Turvey, 2004-2008). The four major types of forensic fraud include: 1) evidence tampering; 2) test result fabrication; 3) perjury; and 4) perjury.

The first type of forensic fraud considered is evidence tampering, which is the falsifying, editing, or amending of evidence. Evidence tampering is usually associated with the crime scene. Television crime drama provides an array of different examples where evidence is planted, taken, or altered at the crime scene by both law enforcement and criminals. Although more difficult to discover and substantiate, evidence tampering can occur at any point in a criminal investigation, including the confines of sterile environments designed to preserve and document physical evidence using scientific methods. Such was the case with forensic Odontologist (bite mark expert) Dr. Michael West. On December 18th and 19th 1993, Dr. West performed two post-mortem examinations of a 23-month old girl who died from drowning in a bathtub while under the care of her mother’s boyfriend (Balkos). The Prosecution alleged the boyfriend raped the little girl, beat her repeatedly, and then drowned her in the bathtub. Dr. West’s findings focused on bite marks that he said matched the dental profile mold (a plaster cast of one’s teeth and bite formations) taken from the mouth of the mother’s boyfriend who voluntarily submitted to the casting process. The only piece of physical evidence heard by the jury was how the bite marks identified on the little girl’s face and elbow matched a mouth cast from the defendant (Balkos). The jury did not, however, know that Dr. West was actually the one responsible for creating the bite mark renderings during his second examination of her on December 15th, 1993. Substantiated by video footage shot as required by the Mississippi morgue where both examinations occurred, the timed footage visually documents Dr. West’s actions during both the first and second examination. Radley Balkos, investigative journalist from Reason Magazine describes the footage of the second examination:

(“Dr. West) repeatedly presses and jars the front bite plate directly onto Oliveaux’s cheek. Over two minutes, he does this 17 times. At 6:57, he starts dragging Duncan’s mold across Oliveaux’s face, beginning near her lips, then scraping the plaster teeth down her face to her jaw. He does this for another minute. West next moves to Oliveaux’s elbow and uses the cast to impress Duncan’s dentition onto an old bruise hospital records show she suffered weeks before her death (Balkos).

The video footage of Dr. West manufacturing inculpatory evidence is a rare event; this type of fraud can be difficult to detect and even more difficult to prove.

The second type of forensic fraud is the fabrication of test results. Usually occurring in a crime lab setting, this type of fraud can include changing results from tests administered or reporting results from testing that never occurred, the latter is frequently referred to as dry-labbing (Pyrek, p. 55). In addition, failure to run proper control tests required to rule out the possibility that the testing process itself does not possess the necessary form of fraudulent behavior. Jacqueline Blake, an FBI biologist who performed tests on DNA from crime scenes during the period 2000 to 2002 admitted to falsifying lab documentation by indicating she completed the proper control tests as required by the lab. Her misconduct went undetected for over two years until a lab colleague noticed results on Blake’s computer were incompatible with the proper processing of control samples (Office of Inspector General, 1997, p. 2).

The third type of forensic fraud is perjury. Knowingly providing false or misleading testimony is perjury. Although the definition is simple, the act can range from blatant to subtle. This type of fraud has become central in the debate about the common courtroom use of expert witnesses, many of whom are accused of building lucrative consulting practices by routinely lying on the witness stand (Barr & Yurman, p. 5). The charge most frequently levied against expert witnesses is that they are hired guns who manipulate the truth to confound or mislead juries (Fisher, p. 6).

Paul Giannelli categorized three common types of misleading expert testimony that influence criminal trials and contribute to unjust verdicts (Giannelli, 2011). The first, withholding information at trial, can be difficult to detect and often poses a serious challenge because the defense attorney possesses incaptious or exculpatory data and actively concealed it from the opposing side. The highly publicized 2011 murder trial of Casey Anthony, an expert witness for the prosecution testified that eighty-six Google searches for the word “chloriform” were performed on Ms. Anthony’s computer before her child was found dead. Just a few days post-testimony, the expert discovered that the software used to extract the information was faulty and the correct number of “chloriform” searches performed was one. He immediately contacted both the prosecution and the police to alert them of the error in an effort to have his testimony disregarded. The trial concluded with no acknowledgement of the error to either the jurors or the defense (Abravanel, 2011).

Giannelli identifies a second type of misleading testimony as the failure to correct overstatements (Giannelli, 2011). Overstatements go beyond the capability of a specific forensic technique and misleads others into thinking a higher degree of certainty is established. For decades, conclusive phrases like “100 percent match” or “it could have only been the suspect’s hair found at the crime scene” were commonplace in court rooms because the limitations of each forensics discipline were unknown. However, now limitations are widely understood and accepted allowing for more accurate analysis through the application of probability statistics.

The final type of misleading testimony Giannelli identifies is information that is presented to a jury during the closing argument of a trial (Giannelli, 2011). In studying trial transcripts of wrongful convictions as referenced earlier in this report, Brandon Garrett and Peter Neufeld cited numerous cases where prosecution made claims in their closing arguments that were not supported by the evidence presented given by forensic analysts, even in cases where testimony from the forensic analyst was deemed valid (Garratt, p. 85). Closing arguments act as powerful summaries of evidence presented over the course of a trial and by mischaracterizing such testimony the prosecution or defense increases the likelihood that a jury will begin deliberating with false impressions.

The final type of forensic fraud is bias. Differing from unintentional bias, fraudulent bias or pro-prosecution bias requires conscious motivation on the part of the forensic worker. Bias of this nature involves law enforcement and/or forensic science personnel providing false impressions.
tiful on CSI-like television shows as everyone is using their unique, specialized talents to collectively prove the home team theory and catch the bad guy. Bias threatens the justice process because it is often systemic or organizational and can exist at all levels of the criminal investigation culminating in a wrongful conviction based on biased information and procedures (Thompson, W. C., p. 1029).

Pro-prosecution bias can be rooted in the powerful incentives inherent to the organization of crime labs. As stated earlier, many forensic examiners are former police officers or FBI agents who think of themselves as police in lab coats and perform their duties accordingly (DiFonzo & Stern, p. 515). Similar to the role of police and investigators, forensic analysts can ostensibly perform their duties while building a scientific case supportive of theories or suspects and suppressing evidence to the contrary. The desire of the forensic scientist to please the prosecutor is the most common explanation offered for forensic fraud (Sedel, p. 897).

REFORMS

In 2005, a state of highly publicized crime lab scandals involving forensic fraud and error prompted repeated appeals for federal intervention to reform the nation’s forensic science systems. Congress authorized the National Academy of Sciences (NAS) to conduct a study entitled “Identifying the Needs of the Forensic Science Community” to be undertaken by a committee of professionals from the law and forensic science community as well as supporting scientific disciplines (National Research Council, p. 2). The final report released by the committee in 2009, titled “Strengthening Forensic Science in the United States: A Path Forward” represented exhaustive research and analysis culminating in the most extensive report on forensics to date, outlining thirteen Recommendations to address the problem of bias and error (National Research Council, p. 24).

The aim of this Recommendation is to substantiate well-known academic claims that all forms of bias can result in fraud and error in forensic workplaces. By acknowledging this fact, the work of standardizing best practices for dissemination can begin. Additionally, Recommendation Five works in concert with Recommendations Seven and Eight that call for mandatory lab accreditation, individual certification of forensic professionals and the implementation of routine quality assurance and control procedures designed to detect fraud and error, respectively (National Research Council, p. 26).

Lastly, NAS Recommendation Eleven seeks to replace existing corner systems with NIFS accredited medical examiner systems. In addition, funding would be expressly designated for improving medical/legal death investigations (National Research Council, p. 30). This Recommendation, would entice the sanction of death investigations to forensic science and medical traditions. The thirteen NAS Recommendations are broad and complex, perhaps to the point of rendering them too massive and expensive to implement. The perception that the NIFS will be just another inefficient, slow federal government bureaucracy is an obstacle to NAS’s proposed reforms. Other leaders from the forensic community differ with the NAS or offer their own insights and strategies to combat forensic bias and error.

Recommendation One proposes the creation of an independent federal entity, the National Institute of Forensic Science, (NIFS) to oversee further development of all forensic science disciplines. This organization would be grounded in science instead of law, operating with skilled leaders who can unify competing voices within the forensic community and promote the interests of all the related disciplines on a national scale (National Research Council, p. 18). This recommendation is the bedrock for all additional recommendations; it establishes a foundation designed to create, maintain and evaluate critically needed solutions for problems that have plagued forensic science for decades.

Recommendation Four removes public crime labs from the administrative control of law enforcement and/or prosecutors (National Research Council, p. 24). NIFS’s recognition that scientific goals are incompatible with law enforcement goals is profound and is, perhaps its most significant advancement to the future of the forensic science community” (Turvey, 2009, p. 6). This recommendation is not a complete solution to the problem of bias; however, it can be a catalyst for the crucial cultural change necessary for scientific principles to more fully govern crime labs.

Recommendation Five tasks the NIFS with fostering research efforts on errors in forensic endeavors and the role of bias in forensic science. After such research is complete, NIFS will be further tasked with creating standard operating procedures designed to minimize both bias and error (National Research Council, p. 24).

The perception that the NIFS will be just another inefficient, slow federal government bureaucracy is an obstacle to NAS’s proposed reforms. Other leaders from the forensic community differ with the NAS or offer their own insights and strategies to combat forensic bias and error. The surest safeguard against fraud and bias in criminal prosecutions is the knowledge among police lab technicians that there is a public defender who will not accept their assertions at face value, who will obtain independent review and retesting of their work (Castelle, p. 3).

CONCLUSION

In a recent interview, Scott Burns, Executive Director of the National District Attorneys Association who represents prosecutors directly in every 97 percent of criminal trials in this country, summarized his position on the increased scrutiny of forensic fraud and error, “This isn’t the first time” (Burns). As he explained his position, he deferred to statistics to formulate an estimated wrongful conviction rate of less than 0.0001 percent or one ten-thousandth of 1 percent. Stipulating that wrongful convictions are the scourge of any justice system, Mr. Burns fully supports efforts to mitigate forensic fraud and error but he cautions against favoring what isn’t broken (Burns).

The only way to definitively know the pervasiveness of forensic fraud and error would require reviewing every case, in every court, in every jurisdiction for at least a decade to ascertain the scope of the problem. Currently, this approach is logistically impossible. However, it is apparent that forensic evidence is vulnerable to insidious forms of fraud and error. More disturbing is the fact that most fraud and error goes undetected, and only by rare circumstances is the discovery made that alerts the justice system of foul play (Castelle, p. 8). The sobering truth of the matter is that if not for the capability of DNA technology, many wrongly convicted people either would still be in prison or would have been executed for crimes they did not commit.

The forensic fraud and error that corrupted their trials would perhaps never be reversed. If these tragic examples represent only the tip of the iceberg as argued by some, it is still an unacceptable compromise of the justice system and provides more than enough justification to permanently remedy the situation by adopting reforms necessary to ensure the integrity of the justice system.

REFERENCES


I introduce:

No matter what the investigation is about, one of the most basic questions is, “who is involved?” The next logical questions are, “who did they know?” and, “with whom did they communicate?” Over the years, methods of communication have changed. With these changes have come different investigative methods to answer these questions. Even with all of these changes, traditional phone calls are still the primary method of communication for most people.

Since 2003, Skype has enabled people to make phone calls with voice, chat, and video using a Voice over IP Protocol (VoIP). In Skype's earlier years, its users could only call other Skype users with an application on their computer (Baet, 2014). Today, Skype is owned by Microsoft which allows its users to make calls to, and receive phone calls from, any telephone in the world using the Skype application on a smartphone, tablet, or computer (Microsoft). Skype is not the only provider of VoIP services, but it does have a quarter of a billion end-users worldwide, which makes it a major player in this area (Wingfield, 2012).

If the subject of an investigation is a Skype user, the investigator needs to be able to obtain communication records from the Skype data. A forensic examination of a Windows computer can reveal the contact information and communication records of a Skype user. Skype stores contacts, chats, and other communication records on the hard drive. However, current Skype forensic tools are able to provide only some of the artifacts that Skype stores; other artifacts are on the server and need to be decoded by hand (Shaffer, Skype Data Experiments).

DIGITAL FORENSICS, COMMUNICATION SYSTEMS AND THE LAW

For many years, investigators have had methods of legally obtaining a subject’s communication records. Under 18 U.S.C § § 3123, law enforcement officers gather pen registers, as well as trap and trace data on telephone lines (US DOJ). Furthermore, investigators can get similar information from cell phone, Internet, or email service providers using the authority granted by Congress in the Stored Communications Act and other laws (Harvard Law Review). Moreover, with a Title III or FISA Writewrap court order, law enforcement can even hear actual conversations (US DOJ).

With a proper subpoena or similar legal court order, Skype will provide law enforcement with registration details provided by the person registering, billing address, a list of all Skype numbers subscribed to by the end-user, historical financial transactions, Skype In and Skype Out records of calls to and from the PSTN, SMS data for text messages, historical Skype WebIn and WebOut records, and email and password changes by the end-user (ECSO/Eskype.net). Since obtaining these records requires only a reasonable belief that the records will help the investigation, all law enforcement investigators should be made aware of this capability.

STEVENSON UNIVERSITY

FORENSICS JOURNAL

SkypeTM Artifacts
Karen Lynne Shafer

While the investigator will still serve court orders on the service providers to obtain transactional records, it is important for the investigator, as well as the forensic examiner, to understand what data the service provider stores and what data is stored locally on the device, especially with newer technology like Skype.

VOIP

VoIP is also known as Internet Telephony, is sending voice data in real-time across a TCP/IP network, such as the Internet. VoIP uses either a computer or a handset to break the voice data into packets and then transmit them over the IP network (EU: Economist Intelligence Unit).

Skype is not the only VoIP service in use today. In fact, many people do not even realize that what they consider their “landline” is actually a VoIP telephone. Many ISPs offer bundled telephone services, which are in fact running across the Internet connection, not the PSTN system. Both MagicJack and Vonage are VoIP systems (MagicJack). What makes Skype different from other providers is that Skype service is free and the content is encrypted.

SKYPE

A Skype user can call, chat, or video conference with any other Skype user at no cost. Skype offers premium services such as calling to and from a phone, SMS text messaging, and call forwarding. These services are offered on a pay-as-you-go or subscription basis. Skype users can call anyone to call them from a regular phone. With these more traditional phone features, Skype is competitive with most communication providers (Skype, Inc.). The Skype application is also available for Windows or Apple computers, most tablets and smartphones (Molnar, et al.).

According to the Skype website, Skype transmissions across the network are encrypted and each user is verified by a digital certificate (Skype, Inc.). The ability of users to communicate with anyone in the world via an encrypted communications network, at no cost, makes Skype a popular service for anyone wishing to hide their phone calls (Dusqujois, Burschka and McLaughlin). Peer-reviewed journal articles exist on the encryption strength of Skype, as well as on detecting and unscrambling Skype network traffic. This paper will focus on the forensic data artifacts stored in the hard drive and RAM of the Skype user’s Windows-based machine, as well as provide information on what data is stored on the Skype servers.

EXPERIMENTS

To determine what data evidence artifacts remain on the hard drive, several experiments were conducted to generate known Skype data using a Windows 7 computer (SUBJECT). Windows 7 was chosen.
as the research operating system because as of October 2012 it is the current version of Microsoft Windows (Microsoft Corporation).

At the start of the experiment one, Windows 7 was installed on a forensically clean hard drive. Skype version 5.10 [FREE] was installed and a user created and named “joseph.skyperuser” to access the Skype website (Skype version 5.10). The research drive was imaged at this stage [INSTALLATION], in order to determine the default settings and installation files for Skype.

For experiment two, two additional Skype users were created on additional Windows 7 computers. All three computers logged into the Skype application, and multiple Skype sessions were conducted. Skype features such as chat, voice calls, video calls, file transfers and group chats were used. Contact information was sent and received. Unique network text strings such as “ZNCBFRM” and “MBRXXC” were sent during the chat sessions to facilitate later searching. The SUBJECT computer was forced into hibernation in order to generate a “hiberfil.sys” file on the SUBJECT hard drive.

For experiment three, the RAM of the SUBJECT computer was captured twice during the Skype sessions. Three RAM captures were searched for residual Skype data to determine if any useful artifacts remained in RAM.

Advanced and paid features of Skype were used in experiment four. The user called phone lines, cell phones, and sent SMS text messages. Call forwarding was enabled, so that when the Skype user was offline, the phone calls received were automatically forwarded to a telephone number. Voicecalls was named on and several messages were left. The Skype data of both sides of these sessions was imaged and processed.

During the experiments, a hand-written log, as well as a photo log, of the data sent and received was kept. At the end of experiments two, three and four, the SUBJECT computer was again forensically imaged. The INSTALLATION and EXPERIMENTS images, as well as the memory captures, were processed using a general forensic tool, in this case Access Data’s FTK Lab version 3.3 (Forensic Toolkit Lab v3.3).

INSTALLATION ARTIFACTS

The default installation location for the Skype program is “[OS Drive]/Program Files or Program Files (x86)/Skype.” The Skype program subfolders are “Phone”, which contains the skype.exe application, “Installation” and “Updater” (Shafer, Skype Data Experiments). The Skype Windows Registry is a database that tracks all information and settings for an installation of Windows (Honeycomb). Relevant artifacts in the software Registry file are the installation date and time, the installation folder and version number. The Skype updater service is referenced in the system Registry key, along with firewall rules. The Skype user name are not found in the Registry (Shafer, Skype Data Experiments). The Registry and its backups will provide information on whether Skype was ever installed on the computer, when it was installed and what version was installed (Shafer, Skype Data Experiments).

SKYPE REGISTRY DATA

Another location for Skype installation and data artifacts is the Windows Registry (Shafer, Skype Data Experiments). The Windows Registry is a database that tracks all information and settings for an installation of Windows (Honeycomb). Relevant artifacts in the software Registry file are the installation date and time, the installation folder and version number. The Skype updater service is referenced in the system Registry key, along with firewall rules. The Skype user name are not found in the Registry (Shafer, Skype Data Experiments). The Registry and its backups will provide information on whether Skype was ever installed on the computer, when it was installed and what version was installed (Shafer, Skype Data Experiments).

The central SQLite database file for each Skype user is “main.db.” This database contains tables that store account settings, alerts, and contacts. It also tracks voice and video calls, chat or SMS message sessions, file transfers, and voicemails. In the accounts table, for instance, the Skype user name, phone numbers, email addresses, Skype balance, as well as the general account options are stored (Shafer, Skype Data Experiments).

LOCATIONS OF SKYPE DATA

The central SQLite database file for each Skype user is “main.db.” This database contains tables that store account settings, alerts, and contacts. It also tracks voice and video calls, chat or SMS message sessions, file transfers, and voicemails. In the accounts table, for instance, the Skype user name, phone numbers, email addresses, Skype balance, as well as the general account options are stored (Shafer, Skype Data Experiments).

The locations for the Skype program include: “C:\Program Files\Skype\skype.exe”, “C:\Program Files\Steam\steamapps\common\Skype\skype.exe”, and “C:\Program Files\Steam\steamapps\common\Steam\steam.exe” (Shafer, Skype Data Experiments).

The date and time in the tables are stored in UNIX or Epoch time (Shafer, Skype Data Experiments). Epoch time is the number of seconds elapsed since January 1, 1970. Therefore the entry “1349239523,” in the “timestamp” field seen in Figure 3, can be converted to “9/20/2012 14:29:11 GMT” (Foggi).

FIGURE 3: Explanation of Messages Table

Each Skype user has a full name, a user name, and a hexadecimal account number that is used by the Skype service. The messages table shows this hexadecimal account number in the “chatsname” field (Shafer, Skype Data Experiments). During a forensic examination of multiple computers, searching the other computers for any of the hexadecimal account numbers found on computer one may show partial chats in unallocated or free disk space. A snapshot can be sent to Skype for the account information using any of these Skype IDs.

VOICE AND VIDEO CALLS

Unfortunately, unlike the chat messages which are stored by defaults, the contents of Skype voice or video calls is not recorded. In normal call sessions, Skype keeps both transactional voice and video calls records in the same table. The date and time of the calls, duration, participants and video settings, as well as other data, is kept in the calls table of “main.db.” Figure 4 displays part of the calls table. The “duration” field is in seconds, and therefore the entry “219” can be converted to three minutes and 39 seconds. The “is_incoming” field will contain either a zero or one; one indicating true. Therefore, in Figure 4, the calls in the second and fourth columns are outgoing calls.
and the call in the third column is incoming. The "host_identity" and "current_video_audience" fields show the participants in the call, but the "is_incoming" field needs to be referenced to determine who was calling whom. The date and time that a call begins is stored as epoch time in "begin_timestamp" (Shafer, Skype Data Experiments).

**FIGURE 4:** Explanation of Calls Table.

**SMS MESSAGES**

As a paid feature of Skype, users may send SMS text messages to a cellphone. They can even record a cellphone number to receive SMS replies (Skype, Inc.). Skype tracks the phone number the SMS text message was sent to, as well as the message itself, in both the "message" and "SMSes" tables of "main.db." Figure 6 shows the relevant fields of the "message" table. In the "charname" field, the sender of the SMS message, in this case "skyperuser," is displayed, along with the phone number the SMS was sent to, as well as the SMS message text. Furthermore, each SMS message, and phone number that the SMS was sent to, is again stored in "main.db." With multiple locations for target phone numbers and SMS messages, the chance of finding this information in deleted or carved spaces on the hard drive increases.

**FIGURE 5:** Explanation of Transfers Table.

**VOICEMAIL**

Each voicemail recording is stored in the Skype user's "voicemail" folder and named "V#.dat." The data file name can be found in the "path" field of the "voicemails" table, in "main.db." Therefore in Figure 7, for the voicemail received on 10/13/12 at 11:27 am, the corresponding "dat" file is named "V1350142942M1M10000001196D264683532.dat." Both voicemails received by the user, as well as voicemails left by the user, are recorded by Skype. The "type" field keeps track of whether the voicemail was received, "1" or left, "3." The greeting heard when a voicemail is left will be displayed as type "2." The "timestamp" field holds the epoch date and time of the voicemail. The actual content of the "dat" voicemail file is proprietary and Skype must be used to listen to the call (Shafer, Skype Data Experiments).

**FIGURE 6:** SMS Messages.

**FIGURE 7:** Explanation of Voicemail Table.

**CALL FORWARDING**

Another paid feature of Skype is call forwarding. Skype users turn on call forwarding at the Skype website by entering an alternate number for forwarding purposes. When they are off-line, all Skype calls are automatically forwarded to a phone number (Skype, Inc.). It should be noted that call forwarding overrides voicemail. The person calling will receive a message on the screen that their phone call is automatically being forwarded. Skype changes the person who the call is forwarding to, should the caller accept the forwarded call. The caller ID displayed on the phone receiving the forwarded phone calls was 661-748-0246, however more experimentation, over a longer period of time, would be needed to see if this was the only caller ID number displayed by forwarded calls (Shafer, Skype Data Experiments).

In reviewing the "main.db" tables of the user who had call forwarding turned on, no indication the call forwarding could be located. The phone call is listed as a missed call. In the accounts table however, the "official_callforward" field contains a "0.60.180555551212" when call forwarding was turned on. When call forwarding was turned off, the field changed to "[NULL]." Having no record of the previous call forwarding settings (Shafer, Skype Data Experiments). Since no indication of call forwarding is seen, the investigator should be made aware that call forwarding could have been activated, thus, the call in question may have been received.

**DATA IN RAM MEMORY**

Fragments of chat conversations, user contact information, user avatars and files transferred were found in the RAM Memory captured during experiment three. In Figure 8, the text chat "search term point," which had been sent twice by "joseph skyperep" to "three skyperep," is shown labeled number 1. The image in the background shows the actual chat in progress. As previously mentioned, the hexadecimal Skype user information can be used to search for Skype data fragments, see Figure 8 label number 2 (Shafer, Skype Data Experiments). Once the user deletes a voicemail, the corresponding "dat" file is deleted. These files may be found among the deleted files on the computer (Shafer, Skype Data Experiments).
During a forensic examination for Skype data, it is important for the examiner to look for data in all possible locations. On scene respondents should be made aware of the importance of capturing the RAM of computers that are on, before this important data is lost forever.

**AUTOMATED SKYPE FORENSIC TOOLS**

As discussed previously, Skype data is mainly stored in SQLite database tables and can be decoded manually. However, with a large amount of Skype data, this could be a time-consuming and tedious process. A standard forensic software suite like Forensic Toolkit, EnCase or Xways, will enable an examiner to find and view Skype data. However, finding Skype data outside of the normal, active, Skype data files, in RAM or in “hiberfil.sys” is more difficult (Shafier, Skype Data Experiments).

Automated tools, specifically designed to decode Skype data, make it easier to present Skype artifacts to the investigator. After an Internet search for Skype tools and discussions with other forensic examiners, a list of automated Skype tools was compiled, including Nirsoft’s SkypeLog View, Sanderson Forensics’ SkypeAnalyzer, Belkasoft’s Skype Analyzer, and Magner Forensics’ Internet Evidence Finder (Shafier, Skype and Digital Forensics). Each of these software programs was tested against the experiment data to determine what artifacts they would decode. When possible, the full version was tested, however in some cases free demonstration versions were tested.

For the testing, each software program’s output was compared to the screen captures and written logs kept during the experiments. Date and times were checked for format and accuracy. A count was made of the number of chats sent and received; number of phone calls sent and received, etc. These were compared with each tool’s output. All the Skype artifacts found during the manual decoding were looked for in the tool’s reports. Table 1 lists all the artifacts available and whether the tool was successful in obtaining this information (Shafier, Skype Data Experiments).

Overall, the tools tested performed as expected. That is, each provided the output its publisher claimed it would produce. The output of these tools was accurate for this limited test data set. The most expensive tools did provide more information, but the low cost and free tools did very well (see Table 1). Special attention should be paid to the time zone information provided on the reports, as this was not always clearly defined by time zone (Shafier, Skype Data Experiments).

**CONCLUSION**

A forensic examination of a Windows computer can reveal the contact information and communication records of a Skype user, but the current Skype forensic tools do not necessarily provide all the artifacts that Skype stores. The answers to those important investigative questions, “who did they know?” and “with whom did they communicate?” may be found in their Skype contacts. Skype’s recording of phone call, message and video call transaction information, such as date, time, and duration, is very much like the pen register data the investigators have come to expect from the phone companies. Important information such as address and banking information can only be found on the Skype servers. The subpoena can be a powerful tool when a subject is a Skype user, and more investigators should make use of this tool to obtain this server data. Records of chat conversations and voicemail records provide the answer to, “what did the subject say?”

There are multiple forensic software programs available to decode the Skype data on a Windows computer. Even without these programs, Skype data may be decoded by hand using standard forensic programs. Because much of these programs decode all the data that Skype stores, forensic examiners should decode the additional data, such as account options, by hand.

**REFERENCES**


LEMR@skype.net. Skype Communications, Inc. 2012. Email.
Karen Lynne Shafer is a Senior Information Technology Specialist Forensic Examiner with the Richmond Division of the Federal Bureau of Investigation. Besides FBI CART certifications in Windows, Macintosh, Cell Phone and Digital Camera forensics, Mrs. Shafer also holds EnCE and IACIS CFCE certifications. She was the Program Manager for the FBI’s CART Digital Forensic Training Program at Quantico, VA from 2002-2004. She has a B.S. in Computer Science from Towson University of Maryland and is currently a student in the Masters of Forensics Studies – Computer Forensics track at Stevenson University.