CFE UPDATE

March-April 2005

Chapter Board of Officers

President: Joseph R. Dervaes, CFE, CIA (360) 710-1545
Member of ACFE Board of Directors, 2003 Cressey Fraud Lifetime Achievement Award Winner, ACFE Fellow, Regent Emeritus, and Distinguished Achievement Award Winner, Association of Certified Fraud Examiners; Audit Manager for Special Investigations, Washington State Auditor=s Office; and, Founding President, Pacific Northwest Chapter/ACFE.
dervaesj@sao.wa.gov, Port Orchard, Washington

Vice-President and Training Director: Norman J. Gierlasinski, PhD, CFE, CPA, CIA 2002 ACFE Outstanding Achievement in Fraud Education Award Winner, and Distinguished Achievement Award Winner, Association of Certified Fraud Examiners; Professor of Accounting, Central Washington University (SeaTac Center) (206) 439-3800, Extension 3825. normang@cwu.edu, SeaTac, Washington

Secretary-Treasurer: Roger B. Gulliver, CFE, CPA, CISA, CBA
President, Gulliver and Associates PS (253) 735-2392; Distinguished Achievement Award Winner; rbg1@mindspring.com, Auburn, Washington

Director-At-Large: Bernadette McBride, CFE, CPA
Senior Investigator/Financial Examiner, Washington State Department of Financial Institutions, Securities Division, (360) 791-8824; Distinguished Achievement Award Winner.
bmcbride@dfi.wa.gov, Olympia, Washington

Director-At-Large: Robert A. Goehring, CFE, CPA
Audit Manager, City of Kent - Finance Department, (253) 856-5262; Distinguished Achievement Award Nominee for 2005; rgoehring@ci.kent.wa.us, Kent, Washington

Association and Chapter Fraud Training and Meeting Dates

Be sure to mark the following calendar year 2005 fraud training meetings on your personal schedule and plan to attend:

April 27, 2005 (Wednesday). Chapter Fraud Training Seminar; Downtown Seattle, at 1000 Second Avenue in a 28th floor conference room of the Washington State Housing Finance Commission. This is the old Key Towers Bank Building; but, the building currently has no name on it. The building is located across the street and one block North of the Jackson Federal Building (corner of Second Avenue and Spring Street). We begin all meetings promptly at 2:30 p.m., hold a 30 minute networking session at 3:30 p.m., and then complete the seminars at 4:45 p.m. The seminar fee is $20 for Chapter members and $25 for non-members.

The Chapter Board of Officers has decided to use a video produced by the Association of CFEs for this training meeting. The title of the video is ABeyond the Numbers@, and the area of concentration is AInterviewing@. The video is a one-hour presentation. Following the video, the Chapter Board of Officers will hold a panel discussion on the content of the presentation, provide interviewing case studies of their own, and receive input on interviewing case studies from the participants. So, attendees should be prepared to actively participate in this event. Come and share your knowledge of case studies from your life experience. You=ll be glad you did!

June 29, 2005 (Wednesday). Annual Chapter Business Meeting and Fraud Training Seminar; Bahama Breeze Restaurant, 15700 SouthCenter Parkway, Tukwila, WA 98188, (260) 241-4448. For reference purposes, the restaurant is located on the Northwest corner of SouthCenter Mall nearest to the intersections of I-5 and I-405. Door prizes will be awarded; but, you must be present to win. The luncheon and continuing professional education for the fraud seminar is free to Chapter members and $15 for non-members. The luncheon begins promptly at Noon, followed by a brief Chapter annual business meeting. The fraud training seminar begins at approximately 1:00 p.m. and lasts for one hour.

The speaker for this meeting will be David Vicente, Anti-money Laundering Specialist from the Taxpayer Education and Communication Unit of the Small Business/Self-Employed Operating Division of the Internal Revenue Service, Oakland, California. The topic will be Anti-Money Laundering Outreach.

July 10-15, 2005 (Washington, D.C.). Association=s 16th Annual Fraud Conference and Exhibition. Register for this conference at www.cfenet.com. The Conference is being held at the Hilton Washington, 1919 Connecticut Avenue, Washington, DC 20009. Hotel rates for the conference are $179 single and $199 double. The meeting times are from 1:00-5:00 p.m. on July 10, 2005, for the Pre-Conference; 8:30 a.m. B 12:30 p.m. on July 13, 2005, and from 8:30 a.m. B 4:30 p.m. on all other days during the Main-Conference and Post-Conference period. The discounted registration fee for Association members is $795 for the Main-Conference. The regular registration fee for non-members is $895 for the Main-Conference. The discounted registration fee for Association Members is $1,225 for the Full Conference. The regular registration fee for non-members is $1,395 for the Full Conference.

Government Highlights of the Conference include:

General Session Speaker James B. Comey, Chair, Corporate Fraud Task Force, U.S. Deputy Attorney General.
General Session Speaker Brian Lamkin, Chief of the Financial Crime Section, FBI.
General Session Speaker, Tim Noonan, Former President, Rite Aid Corporation.
Break-Out Fraud Seminars on Protecting the Public Interest and Fraud Concerning Government:

a. How to Detect Money Laundering, Don Semesky, Chief, Financial Operations, DEA.

b. *Cooking the Public=s Books, Kevin Sisemore, CFE, Fraud Audit Manager, University of Colorado*
c. *Don=t Take Grant Fraud for Granted, Ken Dieffenbach, Special Agent, CFE, U.S. Department of Justice, Office of the Inspector General, Fraud Detection Office.*
d. *Stealing from Big Steel: A vendor Fraud Case Study, Craig Greene, CFE, CPA, Partner, McGovern, Greene, LLP, and David Highlands, Former Director of Internal Audit, National Steel Corporation.*
e. *Eleven educational tracks with more than 60 sessions to choose from.*
f. *Exhibit Hall includes cutting edge anti-fraud tools and services, and highlights the Cyber Café and Career Corner.*

Vice-President Norm Gierlasinski will be the Pacific Northwest Chapter=s official representative at the Chapter Representatives Meeting held in conjunction with the Annual Fraud Conference. He will provide a report to the Chapter on the events of this meeting upon his return.

President Joe Dervaes will attend the ACFE private non-profit corporation=s Board of Directors Meeting held in conjunction with the Conference. He will also attend the Chapter Representatives Meeting, if possible.

August 31, 2005 (Wednesday). Chapter Fraud Training Seminar; Downtown Seattle, at 1000 Second Avenue in a 28th floor conference room of the Washington State Housing Finance Commission. This is the old Key Towers Bank Building; but, the building currently has no name on it. The building is located across the street and one block North of the Jackson Federal Building (corner of Second Avenue and Spring Street). We begin all meetings promptly at 2:30 p.m., hold a 30 minute networking session at 3:30 p.m., and then complete the seminars at 4:45 p.m. The seminar fee is $20 for Chapter members and $25 for non-members.

The speaker for this meeting will be: Frank Walker, CFE, PI, CEC, CBC, BSBE. Frank is a Chapter Member. The topic will be: Selling Fraud Prevention By Persuasion B What CFEs Can Do?

September 20, 2005. Joint Chapter and Seattle Chapter/WSCPA two-hour training meeting. The speaker will be Chapter President, Joseph R. Dervaes, CFE, CIA, Audit Manager for Special Investigations, Washington State Auditor=s Office. Joe is the 2003 Cressey Fraud Lifetime Achievement Award Winner, a Member of the ACFE Board of Directors, ACFE Fellow, Regent Emeritus, and Distinguished Achievement Award Winner at the Association of CFEs. The topic will be Accounts Receivable Fraud using a handout from writings in his By-Line Column, Frauds Finer Points, published in The Fraud Magazine. The meeting is held at the Washington Athletic Club in downtown Seattle from 7:30-9:30 a.m. Additional information on registration procedures will be provided as the information becomes available. Some training information may be available at the WSCPA web-site or by contacting them directly by calling 1-800-272-8273 (Bellevue, WA).

October 17-19, 2005. Joint Chapter and Association of CFEs Fraud Training Classes at the Doubletree Hotel, 18740 International Boulevard; SeaTac (across the street from SeaTac International Airport), (206) 246-8600.

The subject of a one-day class on October 17, 2005, will be Building Your Fraud Examination Practice. The registration fee for this class is $249 for ACFE Members and $299 for Non-Members.

The subject of the two-day class on October 18-19, 2005, will be Communicating the Results of Your Fraud Examination. The registration fee for this class is $595 for ACFE Members and $695 for Non-Members. There is also a $95 savings for early registration.

Note: The Association will provide breakfast pastries, lunch, and mid-morning and mid-afternoon refreshments on each of these training days. Speakers are to be announced at a later date.

December 2, 2005 (Friday). Joint Chapter/WSCPA=s 9th Annual Fraud Conference at the SeaTac Marriott Hotel; 3201 South 176th Street, SeaTac (across the street and up the hill a short distance from SeaTac International Airport). The estimated early registration fee for members of the WSCPA and the Pacific Northwest Chapter is $175 for this conference. There is also a $6 daily parking fee if you drive your car and park in the hotel parking lot. Car pooling is recommended to reduce the nominal cost of parking. Registration and continental breakfast is at 8:00 a.m. The conference begins at 8:30 a.m. and ends at 5:00 p.m. Register directly with the WSCPA by calling 1-800-272-8273 (Bellevue, WA). The conference includes eight hours of continuing professional education credit. The course registration form can also be obtained from the WSCPA=s web site at www: wscpa.org. You must call the WSCPA to actually register for the conference. Ask for Lisa Chin Iwata in the Education Department.

President Joe Dervaes and Vice-President Norm Gierlasinski will co-chair the 9th Annual Fraud Conference. The Chapter Board of Officers is working on the tentative list of speakers and topics for the annual fraud conference (to be announced).

(Uncomfirmed) The speakers for one of four fraud sessions will be Suzanne Sarason and Leslie Pearson, Investigators/Financial Examiners from the Washington State Department of Financial Institutions. The topic will be: Ponzi Schemes. The presentation includes a discussion of a current case study about a recent Ponzi Scheme that was investigated in this state.

Important Chapter Fraud Training Meeting Information for Downtown Seattle Location

All fraud seminars conducted by the Chapter in downtown Seattle are held at this location.

We meet at 1000 Second Avenue in a 28th floor conference room of the Washington State Housing Finance Commission. This is the old Key Towers Bank Building; but,

the building currently has no name on it. The building is located across the street and one block North of the Jackson Federal Building (corner of Second Avenue and Spring Street).

Please pay particular attention to the following rules for visiting our fraud seminar training location in downtown Seattle. Our host, the State of Washington Housing Finance Commission, controls the conference room where our meetings are held and has asked for our cooperation in implementing these security and access rules. The Chapter Board of Officers appreciates your cooperation with these requirements.

_ First, building security. The staff has asked us to go to the Commission=s main offices on the 27th Floor and sign-in with the receptionist before going to the 28th Floor conference room for the fraud seminar. A visitor=s badge will be issued to you. Please turn-in this visitor=s badge in the conference room before departing the building. The Chapter will turn-in all visitor badges at the end of the day.

_ Second, the time of our fraud seminar. The staff has asked up to depart the facility promptly because their duty day ends at 5:00 p.m. Therefore, we will begin all meetings promptly at 2:30 p.m., hold a 30 minute networking session at 3:30 p.m., and complete all fraud seminars at 4:45 p.m. sharp. Visitor badges will be collected at this time.

If you=re looking for parking, Special Events parking rates ($5) apply for the parking garage at Benaroya Hall, just two blocks north of the training facility on Second Avenue.

(1) National Fraud Awareness Week

The Pacific Northwest Chapter/ACFE once again has been listed as a supporter of National Fraud Awareness Week (July 10-15, 2005) sponsored by the Association of CFEs.

As you know, fraud affects businesses and government entities of all shapes and sizes, making the prevention and detection of it everyone=s concern. Today fighting fraud is a challenge for all of us.

To further support the anti-fraud community, six years ago the ACFE created National Fraud Awareness Week, a week dedicated to increasing fraud awareness and advancing the global fight against fraud. The ACFE, along with official supporters from the public and private sector, are proactively taking the first step toward curbing fraud by promoting anti-fraud education and awareness. The ACFE encourages professionals around the world to explore ongoing anti-fraud efforts and get educated about the magnitude of fraud, its impact on the economy, how to report it and above all, the steps needed to prevent, detect and deter it.

As a past supporter, our CFE Chapter has established itself as a leader in the community. If any CFE wants to list his/her organization as a supported of National Fraud Awareness Week, simply complete the short online form at www.FraudWeek.com. The organization will send you an Official Supporter CD with

valuable anti-fraud resources, and highlight your organization on the supporters page of the web site. There is no cost to participate in this initiative.

The National Fraud Awareness Week kick-off event is the 16th Annual ACFE Fraud Conference & Exhibition, held in Washington, D.C. July 10-16, 2005. Over 1,500 anti-fraud professionals are expected to attend making it the world=s largest conference of its kind. Visit www.FraudConference.com for more information about the Conference..

(2) 16th Annual Fraud Conference

This is just a reminder notice about a fantastic training opportunity for Certified Fraud Examiners and others interested in the wonderful world of fraud. See complete details about the Conference in the Chapter training schedule listed at the beginning of this newsletter. Our CFE Chapter has been well represented in past years, and we want to continue that tradition again this year. Come join your fellow professionals at the premier fraud conference sponsored by the Association of CFEs. You=ll be glad you did!

(3) CFE Chapter Annual Luncheon and Business Meeting B Location Change

Special Notice: Due to popular demand, the location has been changed for our Annual Luncheon and Business Meeting. The restaurant we were using was unable to provide the space we needed for the meeting.

As a result, your CFE Chapter Board of Officers has selected a replacement restaurant for the June 29, 2005, meeting. It will be held at the Bahama Breeze Restaurant, 15700 SouthCenter Parkway, Tukwila, WA 98188, (260) 241-4448. For reference purposes, the restaurant is located on the Northwest corner of SouthCenter Mall nearest to the intersections of I-5 and I-405. Door prizes will be awarded; but, you must be present to win.

See complete details about this meeting in the Chapter training schedule listed at the beginning of this newsletter. Come join your fellow Chapter professionals and have fun as well. You=ll be glad you did!

(4) Minutes of Semi-Annual Meeting of the CFE Chapter Board of Officers.

The Chapter Board of Officers held its semi-annual business meeting at the Downtown Seattle Training Location prior to the February 23, 2005, fraud training seminar (12:30-2:30 p.m.). Present were Joe Dervaes, Norm Gierlasinski, Bernadette McBride, and Robert Goehring. Roger Gulliver was unable to attend the meeting and fraud seminar due to a prior work engagement. After a call to order by President Joe Dervaes, the following items were discussed and/or acted upon at the meeting:

(a) By unanimous vote, the Board of Officers approved the minutes from its October 13, 2004, meeting.

(b) President Joe Dervaes presented many items representing notice only to Board members. No action was required. They were:

(1) The CFE Chapter Directory was issued to the membership in December 2004. The Chapter=s Annual Recertification Report was submitted to the Association in December 2004. The Distinguished Achievement Award for Bernadette McBride was submitted to the Association in December 2004. It was previously approved by the Board and by the membership and will be presented at the Chapter fraud seminar today. Associate Member Richard Bologna has sent an e-mail welcome letter to all CFEs contained in the Association=s data base. He=ll work on a similar letter for Associates in the near future. Our hope is that this process will result in a significant increase in Chapter membership.

(2) There will be no elections this year. Elections last year were for two-year terms for the Board of Officers (July 1, 2004, through June 30, 2006).

(3) Two new CFE Chapters have been formed in the past year from within our area of coverage. The Montana Chapter formed in 2003, and the Spokane Chapter formed in 2004. Adding the Oregon Chapter from a number of years ago, we now have 3 step-children Chapters that have spun-off from the Pacific Northwest Chapter/ACFE. This is great news!

(4) Two award nomination packages for 2005 were submitted to the Association of CFEs as follows: (a) Pacific Northwest Chapter/ACFE for the Outstanding Chapter of the Year Award; and (b) Dr. Robert E. Holtfreter, CWU, for the Outstanding Association of the Year Award. The winners of these Association awards will be announced at the Annual Fraud Conference (July 11-13, 2004).

(5) The annual Association and Chapter Scholarship Programs have been officially announced. There are 15 Association scholarships of $1,000 each available this year, and 2 Chapter scholarships of $500 each available this year. Vice-President Norm Gierlasinski has sent scholarship notification letters to Colleges and Universities in our geographic area of coverage similar to prior years.

(6) Roger Gulliver will provide the Board with a status report of Calendar Year 2005 dues payments. We plan to use the CFE Chapter Directory (December 2004) as the basis for tracking the appropriate amount of fees each individual should pay for attending Chapter fraud seminars.

(7) The joint Chapter/Association Fraud Training Classes was moved the previously announced March 2005 dates and will now be held at the Doubletree Hotel during the period October 17-19, 2005. President Joe Dervaes has already signed the letter agreement for the classes. The subject of a one-day class on October 17, 2005, will be Building Your Fraud Examination Practice. The subject of the two-day class on October 18-19, 2005, will be Communicating the Results of Your Fraud Examination. The

Association will provide breakfast pastries, lunch, and mid-morning and mid-afternoon refreshments on each of these training days. This is a change from last year where the lunch meal on the last day of the training was not covered by the Association. The Chapter will not need to pay for lunch for Chapter Members who attend these classes. President Joe Dervaes has requested that the joint Chapter/Association Fraud Training Classes be held in August next year.

(8) The Chapter will be jointly supporting two fraud training classes sponsored by the Seattle Chapter/WSCPA in Calendar Year 2005. Marty Biegelman, Director, Financial Integrity Unit, Microsoft Corporation will be speaking on Tuesday, March 15, 2005 (7:30-9:30 a.m.), on the topic of ABuilding a Fraud Prevention Culture. President Joe Dervaes will introduce him. President Joe Dervaes will be speaking on Tuesday, September 20, 2005 (7:30-9:30 a.m.), on the topic of AAccounts Receivable Fraud@. Chapter member Caroline Walker coordinated these joint training programs for us.

(9) The Membership of the Association elected Marty Biegelman and Joe Dervaes as 2 of the 5 new members of the ACFE private non-profit corporations (c3 and c6) Board of Directors in October 2004. They attended the first meeting in Austin during the period December 15-16, 2004. The Articles of Incorporation and By-Laws were approved for the corporations and will be submitted to the State of Texas and the Internal Revenue Service for approval. However, the Board of Directors was not formally constituted at this meeting. This event will occur at an undisclosed future date, probably in conjunction with the approval of the corporations and the reorganization from a for-profit corporation to a non-profit corporation sometime late in 2005. The approval process will probably take all of 2005. There will be a lot of behind the scenes work and planning taking place in order to make all of this happen on schedule.

(c) The Board discussed nominees for the Chapter=s 2005 Distinguished Achievement Award. By unanimous vote, the Board recommended that Robert A. Goehring, CFE, CPA, Director-At-Large, receive the award this year for his outstanding service to the Association, the Chapter, and the community. This recommendation will be presented to the membership for approval at our annual business meeting in June 2005.

(d) By unanimous vote, the Board approved a recommendation that Norm Gierlasinski and Joe Dervaes be appointed as Chapter Representatives for the annual meeting held in conjunction with the Annual Fraud Conference in Washington, D.C. during July 2005, and that the Chapter pay $500 towards the expenses of Norm Gierlasinski to attend the meeting. The Association will pay all expenses for Joe Dervaes since he will be attending a Board of Directors meeting held in conjunction with the Annual Fraud Conference. The Norm Gierlasinski will make a report of the meeting after the conference that will be published in the Chapter newsletter.

(e) By unanimous vote, the Board approved a recommendation that Joe Dervaes purchase door prizes for the annual business meeting in June 2005 (5 gift certificates for $25 each to Borders Books).

(f) The Board discussed speakers for the remaining fraud presentations in Calendar Year 2005. Speakers have been confirmed for all meetings except for the April 27, 2005, fraud seminar and the joint Chapter/WSCPA Annual Fraud Conference in December 2005. The Board decided to use an Association of CFEs video entitled ABeyond the Numbers@ for the purposes of this meeting. After the video on interviewing, the Board will act as a panel to discuss the video content, to provide interviewing case studies of their own, and to receive input on interviewing case studies from the audience. Many options for speakers at the Annual Fraud Conference were discussed. The Board will begin making contacts to find four speakers (two-hour blocks of time) for the one-day Conference. Specific assignments were made during the meeting.

(g) The Board also discussed a proposal by Bernadette McBride that the Chapter participate in providing fraud training outreach into the community in the future. The Board will begin working on this project in the coming year, and will solicit input from the membership on ways to accomplish this and for assistance in making it happen. Suggestions included civic organizations, senior citizen groups, AARP, the Attorney General=s Office Consumer Protection Division, the Washington State Patrol=s Identity Theft Unit, the Washington State Department of Financial Institutions, the Washington Society of Certified Public Accountants, the Internal Revenue Service=s VITA Program, etc. One way to do this is to have the Chapter sponsor the events, with active and retired Chapter members making the presentations. This alternative would be labor intensive for our Chapter. Another way to do this is to develop the fraud materials and then work with existing community outreach programs of other organizations by having them present the material. This alternative was much preferred by Board Members, especially at first as we begin this new outreach program.

(h) Chapter Board Members perform registration duties at the joint Chapter/ACFE two-day and three-day training classes each year. The Association grants the Chapter two free participant registrations for this work and one free complimentary participant registration for each event. Chapter President Joe Dervaes attends these training classes for free because of his duties on the Association=s Board of Directors. This means that if all Board Members want to attend the joint Chapter/ACFE training classes, one individual would have to pay a registration fee. In the past, the Chapter has paid the registration fee for this Board Member. Similarly, Chapter President Joe Dervaes and Chapter Vice-President Norm Gierlasinski perform co-chairman duties at the joint Chapter/WSCPA one-day Fraud Conference each year. They attend the conference for free. This means that if all Board Members want to attend the joint Chapter/WSCPA Annual Fraud Conference, three individuals would have to pay a registration fee. In the past, the Chapter has paid the registration fee for these Board Members. By unanimous vote, the Board approved a recommendation that the Chapter again pay for the registration fees for any Board Member who is unable to attend either the joint Chapter/ACFE training classes or the joint Chapter/WSCPA Annual Fraud Conference for free.

The semi-annual Board meeting was adjourned by Chapter President Joe Dervaes, and members then attended the Chapter fraud seminar.

(5) Other Training Opportunities

The Pacific Northwest License, Tax, and Fraud Association will hold its annual conference from May 3-5, 2005, at the Red Lion Hotel in Vancouver Washington.

The Keynote speaker will be Rob McKenna, WA Attorney General. Seminar speakers and topics include: David Myers: New Trends and Detection of Counterfeit ID; Marty Biegelman (Chapter Member): Beyond Compliance: Building a Fraud Prevention Culture; Jason Moulton: Private-Public Partnerships: Making it Work!; Ward Clapham, RCMP: Cutting Edge Leadership for the 21st Century; Chuck Whitlock: Fraud Schemes of Today and Tomorrow; Scott Wagner: How to Recognize Fraud in Workers Compensation Claims, Identity Theft, and Money Laundering Fraud; Tom Wendel: What to do if you are Sued--TORT Cases, Lawsuits; Scott Wagner: Current Trends in Vehicle Theft, Vehicle Cloning, and Chop Shop Operations; and, Bill Tufts: Interviewing.

Find out more about this training opportunity by visiting the Association=s web-site at: www.pnltfa.com.

(6) Phishing News

The following article on personal security concerns was published in the Tacoma News Tribune newspaper on Sunday, January 30, 2005. The title is Fraudphobic? Check relatives, not your e-mail, and the sub-title is Survey surprise: Most identity theft takes place the old-fashioned way B getting your wallet stolen. Online fraud ranks far behind. The author of the article is Mindy Fetterman, Gannett News Service.

Identity theft is less likely to happen online than through traditional means, like losing or having your wallet stolen, according to a new survey.

And when the identity of the thief is known, it=s more likely to be one of your relatives.

There were 9.3 million new victims of identity fraud in 2004, or 4.3 percent of the US. Adult population, according to the 2005 Identity Fraud Survey Report. It was released by the Council of Better Business Bureaus and Javelin Strategy and Research. The survey found:

Computer crimes accounted for 11.6 percent of identity theft in 2004, versus 68 percent from paper sources.

The average loss for online identity theft was $551, versus $4,543 from paper.

Family members, friends, and neighbors make up half of all known identity thieves.

Computer theft is way down the list, said James Van Dyke of Javelin Strategy in Pleasanton, California. Doing financial transactions via computer worries Americans, he said, because it=s the great unknown. But, it=s not where your primary risk from fraud is.

Computer identity theft can occur when fake e-mails claiming to be from your bank or credit card company warn you that there has been a problem with your account and you need to log on to the attached link.

This phishing can look like the real thing, but it=s sending you to a bogus site. You won=t know that you=re e-mailing a teenager=s bedroom somewhere with your private information, Van Dyke said.

Only 2.2 percent of identity fraud comes from viruses or hackers; 1.7 percent from fake 3-mails.

The biggest risk for identity fraud is from the old-fashioned theft of your wallet or paper records from your trash. And from people who know you.

People who are close to you can set up known accounts and have the information sent to a new address, Van Dyke said. So the fraud goes on longer and is harder to discover.

Hispanics and African Americans are twice as likely as Asians or whites to experience the most serious fraud, where a thief uses information to set up new bank or credit card accounts.

The Better Business Bureaus and Javelin Strategy did a telephone survey of 4,000 Americans and found 509 who had suffered identity theft. They then questioned those people extensively.

The independent survey was paid for by a group of credit card companies and banks, including Check Free Services, Visa, and Wells Fargo Bank.

Note from Newsletter Editor and Chapter President Joe Dervaes:

A professional friend of mine sent me the following e-mail that his son received the week before this article was published. It=s a good example of what is happening. First comes the phishing e-mail that was received:
Dear (Bank) customer. We recently reviewed your account, and suspect that your (Bank) Internet Banking account may have been accessed by an unauthorized third party. Protecting the security of your account and of the (Bank) network is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features. To restore your account access, please take the following steps to ensure that your account has not been compromised. 1. Logon to your (Bank) Internet Banking account. In case you are not enrolled for Internet Banking, you will have to use your Social Security Number as both your Personal ID and Password and fill in all the required information, including our name and account

number. 2. Review your recent account history for any unauthorized withdrawals or deposits, and check your account profile to make sure n changes have been made. If any unauthorized activity ahs taken place on your account, report this to (Bank) staff immediately. To get started, please click on the link below: (link not provided here). We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire (Bank) system. Thank you for your prompt attention to this matter. The (Bank) team.

Next comes the phishing response from the (Bank).

Thank you for contacting (Bank).

We are aware of recent phishing scams targeting our customers. Most of the scams involved the use of fraudulent email message which appear to be from your bank or another trusted business. The email may employ fraudulent web sites to trick people into sharing personal financial information, such as account numbers, passwords, Social Security numbers and other date.

We would like to assure you that (Bank) was not compromised and we do not send email messages or make phone calls asking for your personal financial information.

When we learn of phishing scams, we work aggressively with law enforcement agencies to investigate them and shut down the fake web sites. To do your part to keep your information safe, please remember to:

Be suspicious of emails with urgent requests for personal financial information.
Do not fill out forms in email messages that ask for personal financial information.
Do not reply to email messages that ask for personal financial information.
Avoid using links in email to get to web pages, especially if you suspect a message might not be authentic.
Ensure that you only use secure web sites to submit credit card or other sensitive information.
Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.

For more information regarding phishing and protecting your personal information, visit our web site at (Bank site). Please do not reply to this email. Thank you (Bank).

Finally, comes the answer.

As I told my professional friend, just tell your son to decide not to play when he receives messages similar to this. Learn how to use the delete function on your computer and get on with live. Remember, your bank will never send you a message like this asking for any of your privacy information to be provided in order to respond. They already have the information on file. We all should adopt this philosophy to avoid becoming a fraud statistic. And, remember, it can often take a decade or so to correct to credit history after you have become a victim of identity theft. It=s ugly business. My best advice is to do all you can to avoid the event in the first place. Good luck!

(7) Other Fraud News

The following fraud article appeared in the Tacoma News Tribune on March 10, 2005. The headline was: AKeep bad guys out of your PC@. The subtitle was: ADon=t think you=re safe from hackers unless you use these four ways to foil them.@ The author was: Heather Newman from the Detroit Free Press. Here=s the article.

It=s a spamdemic. In a survey the National Cyber Security Alliance conduced with America Online last year:

!? 63 percent of those polled said they=d gotten a virus on their computers.

!? More than half of those polled said they had been attached by spyware programs (which track passwords and other sensitive information you type) or adware programs (which flood your computer with advertising pop-up windows). Seven in 10 computer users are victims of cyber break-ins each year. You should buy a firewall and turn your computer off when not using it.

Hacking is only hilarious when it happens to a Hilton.

If someone broke into your computer, they probably wouldn=t get Eminem=s phone number (as hackers who got into T-Mobile=s phone system most likely did from socialite Paris Hilton=s phone book last month).

But they could get things that are much more valuable to you:

!? Your financial information.

!? Your passwords to sites and programs.

!? Your e-mail address to deluge you with spam.

While it=s unlikely that rings of hackers would target you specifically, you still need to take precautions if you operate a computer that=s connected to the Internet, especially if you have a fast, always-on connection like a cable modem or DSL link.

While hackers might not go out of their way to target you, they=re always generically sniffing for opportunities to mess with people=s data B and you might be more vulnerable than you think.

Think it can=t happen to you because yo9u=re not a big business like Bellevue-based T-Mobile or a celebrity like Hilton? Think again.
The National Cyber Security Alliance, based in Washington, D.C., estimates that seven in 10 Americans who go online are the victim of a cyber security or privacy incident each year.
Here are four things to do:

1. Build a wall of defense.

Your first and biggest line of defense is a firewall. That=s a program or piece of hardware B both have the same function, though they operate differently B that stops information requests from coming into your PC that you didn=t authorize. They also stop the flow of data into and out of your PC unless it was a site that you requested to see.

Hardware firewalls, which are typically built into routers that hook up to your cable modem or DSL adapter, are the best choice for fast Internet customers. They provide strong support, even stealthing the ports of communication hackers use B meaning that outsiders don=t know that those ports to your PC exist.

Consider the Netgear line of routers, but most of the top brands serve the same function. It=s worth it to use a router B even if you don=t have multiple PCs or a home network B if you leave your computer on a lot.

2. Turn off your computer.

It=s hard to hack your PC if it=s not on. If you don=t have a hardware or software firewall, you can reduce B though not eliminate B the risk of unauthorized intrusions by turning it off when you=re not using it.

Check your owner=s manual./ Some PCs are set to turn themselves on when the network card that connects to the Internet detects activity. You=d want that option turned off.

3. Stick with dial-up.

Yes, it sounds odd to stick with an outdated link to the Web. But software firewalls are the best bet for dial-up customers because you don=t use your Internet connection as often and because it=s harder for hackers to find you when you do.

Unlike always-on Internet connections, dial-up users get assigned a different Internet address every time they call in. Just as people who make crank phone calls can=t find you if you don=t have a phone number, it=s a lot tougher for hackers to target you without a consistent Internet address.

4. Watch what you load.

Start worrying about the second source of access to your machine B programs you load on your hard drive, accidentally or on purpose. A particular danger is adware or spyware, programs that gain access to your machine through a Web site or an e-mail.

For instance, you might run across a pop-up window that looks just like a system error that requires your attention. But it=s no error B it=s somebody who wants to plant a program on your computer to make it serve up their advertising, or worse.

You need two lines of defense here.

First, you should have a constantly updated anti-virus program (it must be updated regularly, or it won=t detect the new viruses that come out), which would be set to scan incoming and outgoing e-mail to avoid having your PC be used to spam others. Norton AntiVirus and McAfee VirusScan are two common options.

You=ll also need an anti-adware program to keep an eye on software that tracks your keystrokes, serves up ads and otherwise collects information you want to remain private or sends you information you don=t want. Ad-Aware (www.lavasoftusa.com) works well, but there are lots of others.

PACIFIC NORTHWEST CHAPTER
ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

SEMINAR TOPIC B BEYOND THE NUMBERS (April 27, 2005)

The Chapter Board of Officers will serve as a panel of experts to discuss the topic of the Association of Certified Fraud Examiner=s video entitled ABeyond the Numbers@. The Board will interact with the audience in a panel discussion to discuss the Association=s video on interviewing, provide input on interviewing case studies of their own, and accept input on interviewing case studies from the audience.

SPEAKERS

The Chapter Board of Officers is composed of the following fraud experts:

President Joseph R. Dervaes, CFE, CIA, Audit Manager for Special Investigations, Washington State Auditor=s Office, will be absent from this meeting. He will be traveling to a speaking engagement at the Maryland Chapter/ACFE=s Annual Fraud Conference on this date.

Vice-President and Training Director: Norman J. Gierlasinski, PhD, CFE, CPA, CIA; Professor of Accounting, Central Washington University (SeaTac Center). He will be the host for this meeting.

Secretary-Treasurer: Roger B. Gulliver, CFE, CPA, CISA, CBA; President of Gulliver and Associates, PS.

Director-At-Large: Bernadette McBride, CFE, CPA; Senior Investigator/Financial Examiner, Securities Division, Washington State Department of Financial Institutions.

Director-At-Large: Robert A. Goehring, CFE, CPA; Audit Manager, City of Kent - Finance Department.

DATE: April 27, 2005 **TIME**: 2:30 B 4:45 p.m. **CPE**: Two Hours CPE Credit

Location of Training Facility and Parking: We meet at 1000 Second Avenue in a 28th floor conference room of the Washington State Housing Finance Commission. This is the old Key Towers Bank Building; but, the building currently has no name on it. The building is located across the street and one block North of the Jackson Federal Building (corner of Second Avenue and Spring Street). If you=re looking for parking, Special Events parking rates ($6) apply for the parking garage at Benaroya Hall, just two blocks north of the training facility on Second Avenue.

Important Fraud Training Meeting Information for the Downtown Seattle Location is Included in the Bi-Monthly Chapter Newsletter.

Note: We have entered into an agreement with the Washington State Board of Accountancy to meet its continuing professional education requirements.

SEMINAR REGISTRATION FORM (April 27, 2005 B 2:30-4:45 p.m.)

NAME: _____

TITLE: _____

PHONE: _____ FAX: _____

EMPLOYER: _____

ADDRESS: _____

CITY: _____ STATE: _____ ZIP: _____

Please mail registration form with $20 check for members or $25 for non-members to: Pacific Northwest Chapter/ACFE; P. O. Box 215;Auburn, WA 98071-0215. Or, bring your registration form and payment to the Seminar for processing.

SEMINAR TOPIC B BEHIND THE NUMBERS (April 27, 2005)

The Chapter Board of Officers will serve as a panel of experts to discuss the topic of the Association of Certified Fraud Examiner=s video entitled ABeyond the Numbers@. The Board will interact with the audience in a panel discussion to discuss the Association=s video on interviewing, provide input on interviewing case studies of their own, and accept input on interviewing case studies from the audience.

SPEAKERS

The Chapter Board of Officers is composed of the following fraud experts:

President Joseph R. Dervaes, CFE, CIA, Audit Manager for Special Investigations, Washington State Auditor=s Office, will be absent from this meeting. He will be traveling to a speaking engagement at the Maryland Chapter/ACFE=s Annual Fraud Conference on this date.

Vice-President and Training Director: Norman J. Gierlasinski, PhD, CFE, CPA, CIA; Professor of Accounting, Central Washington University (SeaTac Center).

Secretary-Treasurer: Roger B. Gulliver, CFE, CPA, CISA, CBA; President of Gulliver and Associates, PS.

Director-At-Large: Bernadette McBride, CFE, CPA; Senior Investigator/Financial Examiner, Securities Division, Washington State Department of Financial Institutions.

Director-At-Large: Robert A. Goehring, CFE, CPA; Audit Manager, City of Kent - Finance Department.

Many organizations require the **Federal Tax Identification Number** of the Pacific Northwest Chapter/ACFE in order to pay for their employees to attend our fraud training events. The number is: **91-1592735**.

Important Fraud Training Meeting Information for the Downtown Seattle Location is Included in the Bi-Monthly Chapter Newsletter. Check out our web-site at: www.fraud-examiners.org.

John E. Reid and Associates, Inc.; 250 South Wacker Drive, Suite 1200; Chicago, Illinois 60606-5826; telephone: (312) 876-1600 or (800) 255-5747; web-site : www.reid.com; Fax (312) 876-1743.

(1) February 2005 Monthly Web Tip: A Review of Legal Issues Concerning Trickery and Deceit During an Interrogation.

A number of recent cases involving an investigator=s use of trickery and deceit during an interrogation have caused problems in the subsequent trial. In some of these cases the confession was suppressed. These cases have not involved a novel legal argument or radical interpretations of current law. Rather, existing laws have been applied in a predictable manner in situations in which investigators attempted to push the envelope to test the court=s tolerance. This web tip offers a review of some of the legal aspects regulating an investigator=s use of trickery and deceit. An appropriate starting point is to define trickery and deceit from a legal perspective.

Interrogation relies extensively on implication and innuendo. Consequently, almost every interrogation involves some level of at least implied deceit. When the investigator starts out an interrogation by telling the suspect that there is no doubt that he committed the crime, this is oftentimes not a true statement. The investigator may then sit down and explain that the reason he wants to talk to the suspect further is to find out why he committed the crime. Again this is not an accurate description of the purpose of the interrogation. In an effort to establish rapport, the investigator may then state that he believes the suspect is basically a decent and honorable person who acted out of character, which may, in fact, be a false statement.

From a legal perspective, however, the previous false statements merely represent the investigator=s beliefs and, therefore, generally do not fall within the category of behaviors that have been traditionally considered as "trickery and deceit." In this regard, there has been a clear distinction between an investigator stating a false belief (which is generally acceptable) and making a false statement which, if carried too far, could jeopardize the admissibility of a confession. Examples of false statements which the courts may encounter include lying to a suspect by telling him that his partner has already confessed; falsely telling the suspect that if he confesses he will be able to sleep in his own bed that evening; or, showing the suspect a fabricated report indicating that his DNA was recovered from the victim.

When asking the question as to whether or not a particular statement or action may cause a confession to be suppressed, there are a few key cases to keep in mind. The landmark decision concerning trickery and deceit is a U. S. Supreme Court case in which a suspect confessed after being falsely told that his partner had already incriminated the suspect in the commission of the crime(1) . Utilizing the "totality of circumstances rule", the defendant=s confession was upheld. Within the totality of circumstances guideline, the trickery or deceit employed must not shock the conscience of the court or community. An example of behavior that shock s the conscience would be for the investigator to impersonate a defense attorney or clergyman in an effort to elicit a confession.

In the evolution of trickery and deceit laws, the next significant case is Cayward (2). In this case the police typed up a fabricated crime laboratory report which stated that Cayward=s DNA was found during the victim=s autopsy. After reading this report Cayward confessed. The confession was suppressed, not because of either concern listed above, but because of a new rationale. In this instance the investigator crossed the line from making a false statement to manufacturing false evidence. The court was concerned that such manufactured evidence may find its way into court and jeopardize the integrity of the evidentiary system as a whole. The legal guideline stemming from Cayward can be summarized as follows:

A distinction must be made between false assertions (which may be acceptable) to fabricating evidence (which is impermissible.)

In addition to Cayward, other examples of fabricated evidence that have resulted in confessions being suppressed include making an audiotape of an investigator pretending to be an eye-witness (3) to the suspect=s crime and a fabricated crime lab report indicating that the suspect=s DNA was found on a rubber glove recovered from the crime scene (4).

Deliberate falsehoods unrelated to the facts of the crime should be avoided.

While false statements relating to investigative information may be permissible, an investigator should not lie about legal, procedural or administrative issues. Examples of impermissible extrinsic deception include falsely telling a suspect that if he confesses he will be able to sleep in his own bed that

evening, or falsely telling the suspect that if he confesses he will be placed into a witness protection program and not be prosecuted. In a recent case a confession was suppressed when the suspect was told during the interrogation, "If you don=t give us a reason (for the crime) the jury=s never going to hear a reason." (5) This statement, of course was not true and addressed the suspect=s legal defense. As the court pointed out, "The officers in this case might have properly (and truthfully) told Novo, >this is your only chance to talk to us.="

It is the nature of a good criminal investigator to strive to solve a case, ideally with a confession. Furthermore, good investigators are creative not only in their approach to developing investigative leads and evidence, but also in their efforts to elicit the truth during an interrogation. It is at this stage that the investigator must resist the temptation to elicit a confession at any cost. If an investigator tries too hard to elicit a confession and bends the legal guidelines too far, the result is a suppressed confession. The following guidelines are offered to assist an investigator in deciding whether or not a particular false statement offered during an interrogation may jeopardize a subsequent confession:

It is generally acceptable for the investigator to express false opinions during an interrogation.

The exception to this statement is a false belief or opinion regarding legal issues, e.g., "I think since this is your first offense you will probably receive probation," or, "If you did not intend on burning down the whole restaurant, you=re probably just looking at a charge of damaging property." Unless the person conducting the interrogation is a prosecutor with the authority to make charging decisions, legal advice or opinions should not be given during an interrogation.

It is generally acceptable for the investigator to use visual props during an interrogation such as a video or audio tape, a fingerprint card or an evidence bag containing carpet fibers, hair follicles or other evidence.

In preparing these props it is absolutely imperative that the prop would never be mistaken for actual evidence against the suspect. An example of an improper prop would be to take the suspect=s actual latent fingerprint, and adhere it to an evidence card indicating the fingerprint was lifted from the crime scene. This is clearly manufacturing evidence, which is impermissible.

It is generally acceptable for the investigator to make false statements concerning physical or testimonial evidence that implicates the suspect in the crime.

As a precautionary measure investigators must exercise a great deal of caution when making false statements to suspects with diminished mental or intellectual capacities in view of the fact that some of those individuals may be susceptible to pleasing the investigator and may place more credibility on the investigator=s statements than with their own recollections. Similarly, false statements that directly link the suspect to the crime should not be made to a suspect who claims to have no recollections at the time the crime was committed as a result of alcohol or drug intoxication, head trauma, or repression.

The guideline we teach at our seminars is that lying to a suspect should generally be considered as a last resort effort to overcome persistent but weak denials.

If an interrogator is caught in his lie by the suspect he will lose his credibility, and it may cause a custodial suspect to invoke his right to remain silent or ask for an attorney. Furthermore, with electronically recorded interrogations the investigator must be able to articulate his reason at trial for engaging in deception with the suspect.

---

1 Frazier v. Cupp, 394 U.S. 731, 89 S. Ct. 1420 (1969).

2 State v. Cayward 552, So. 2d 921 (Fla. 1989)

3 State v. Patton 826 A.2d 783 (N.J. 2003)

4 State v. Chirokovskcic, 860 A.2d 986 (N.J.Super.2004)

5 Commonwealth v. Novo, 442 Mass. 262, 812 N.E. 2d 1169 (Mass. 2004)

(This article was prepared by John E. Reid and Associates, Inc. as their Monthly Web Tip and was reprinted on our web site with their permission. For additional Monthly Web Tips, go to www.reid.com and click on AHelpful Info@.)

(2) March 2005 Monthly Web Tip: Developing an Interview Strategy.

This introduction establishes the non-accusatory tone of the interview, and also the non-judgmental position of the investigator. The emphasis on being truthful, as opposed to a threatening statement

(such as, "If you lie to me today I will prove that and you will be sorry!") will work to the investigator=s advantage later if it becomes necessary to interrogate the suspect.

The first couple minutes of the interview should consist of non-threatening background questions such as the spelling of the suspect=s name, his address, marital status, job duties, etc. These questions allow the investigator to establish the suspect=s behavioral norms within the areas of eye contact, communication style and general nervous tension. In addition, these initial questions allow the investigator to establish a rapport with the suspect.

The issue under investigation may be introduced by asking the suspect, "Tell me everything you know about (the issue under investigation)." Regardless of the suspect=s answer to that question, it is very important for the investigator to first precisely define the issue under investigation and then ask the suspect whether or not he committed the crime. The following is an example of this in a date rape case:

"Jerry, Linda Jones has reported that last Saturday evening you undressed her and forced her to have sexual intercourse with you by striking her with your hand. If you did do that our investigation will clearly indicate that. On the other hand, if this did not happen it will show that as well. Before we go any further, let me ask, did you force Linda to have sex with you last Saturday evening?"

The reason it is important to precisely identify the issue under investigation is so that the suspect knows whether or not he is innocent or guilty of that issue which, in turn, will affect the validity of his behavior during the interview. Consider that Linda Jones had consensual intercourse with the suspect but that the two of them used cocaine that night. If the investigator is vague in his questions such as, "Jerry, did you do something wrong with Linda last Saturday?" the suspect may exhibit very misleading behavior during the interview.

One reason it is important to ask a suspect, early during an interview, if he committed the crime is because innocent suspects are anxious to let the investigator know that they did not commit the crime. However, if the investigator does not allow the innocent suspect to tell the truth, this may result in increased anxiety which could be interpreted as deceptive behavior. The second reason to directly ask a suspect if he or she is guilty of the crime, is to heighten the suspect=s level of motivation during the interview. On the other hand, if the investigator skirts around the issue and avoids sensitive areas, the innocent suspect is not motivated to convince the investigator that he did not commit the crime. Similarly, a guilty suspect may not be motivated to conceal the fact that he is lying. When a suspect=s level of motivation is low, behavior symptom analysis can be very unreliable.

Developing Information Concerning Investigative Leads, Opportunity and Access

After asking the suspect if he committing the crime it is often appropriate to ask some preliminary questions to address guilty knowledge, complicity or general theories of the crime:

"Do you know for sure who did (commit the crime)?"

"Who do you suspect may have (committed the crime)?"

"Is there anyone you can eliminate as a suspect?"

At this point during the interview the investigator may want to elicit specific investigative information. Examples of possible investigative questions include:

"Tell me everything you did last Saturday night between 8:00 and the time you fell asleep."

"Describe your relationship with Linda Jones."

"What was Linda=s mood when she left your apartment on Saturday?"

"Tell me everything about preparing the deposit last Friday afternoon?"

"Did anything unusual happen while you were making up the deposit?"

"Do you have the combination to the safe?"

Developing Attitudinal Information

Truthful and deceptive suspects form very different and predictable attitudes toward the interview as well as the issue under investigation. At some point the investigator will want to ask specific questions to draw out these attitudes. Examples of questions designed to do this include:

"How do you feel being interviewed concerning (issue)?"

"Who would have had the best opportunity to (commit crime) if they wanted to?"

"Do you really think (the crime was committed)?"

"What do you think should happen to the person who (committed issue)?"

Developing Information Concerning Motives and Propensity

One block of interview questions should explore the suspect=s motives and propensity. If the crime is financially motivated it would be appropriate to discuss the suspect=s current financial status. If the circumstances of the crime appeared to be linked to substance abuse, it would be appropriate to ask the suspect about his use of alcohol and illegal drugs. To evaluation propensity to commit the crime, the following questions may provide insight:

"What is the closest thing to (issue under investigation) that you=ve ever done?"

"Have you every thought about (committing the crime)?"

"Tell me why you wouldn=t (commit crime)?"

"Have you ever been approached by anyone asking you to (commit crime)?"

"Have you ever been questioned before about (issue under investigation)?"

Developing the Suspect=s Explanation for any Evidence

If there is physical or testimonial evidence pointing to the suspect=s possible involvement in the crime, the investigator may want to bring this up during the interview. On the other hand, if the investigator knows that the suspect will be eventually interrogated, often it is beneficial to wait until the interrogation to bring up actual evidence of the suspect=s guilt.

Developing Information About the Suspect=s Confidence

During a non-accusatory interview innocent suspects are confident they will be believed whereas guilty suspects are worried about getting away with their crime. The following questions are designed to assess the suspect=s confidence during the interview:

"When Linda says you slapped her is she lying?"

"Can you think of any reason why someone would name you as the person they suspect?"

"Once we complete our investigation how will it come out on you?"

"Can you think of any reason why the surveillance video would show you inside the vault last Friday afternoon?"

Concluding the Interview

Once all of the relevant information from the suspect has been elicited, the investigator should step out of the interview room, review his interview notes and other evidence collected in the case and make one of three decisions. The first is that the suspect is telling the truth and can be eliminated from further suspicion. Under this circumstance, the investigator should return to the interview room and say something like the following, "Tom I=ve covered everything I need to cover with you. Thank you for coming in. If I need to talk to you further I=ll let you know." A second possibility is that the investigator decides, based on the suspect=s behavior and the evidence, that the suspect is probably guilty of the crime. Under this circumstance, the investigator would return to the interview room and start the interrogation.

In some situations, following the initial interview the investigator may not be able to make a determination of the suspect=s probable guilt or innocence. In other cases, even though the investigator is quite certain of the suspect=s guilt, he may not want to interrogate the suspect at that time. Under these circumstances the investigator would return to the interview room and tell the suspect something similar to the following, "Bill, thank you for coming in today. We are in the process of talking to other people and waiting to get results back on some forensic evidence and it may be necessary for me to talk to you again. You=d be willing to come back and talk to me, wouldn=t you?" In conclusion, an investigator often has only one opportunity to conduct a formal interview of a suspect. To maximize the amount and quality of information learned during the interview, a specific structure should be used. The issue under investigation should be clearly defined and a series of prepared questions should be asked to develop investigative information and behavior symptoms of truth or deception.

(This article was prepared by John E. Reid and Associates, Inc. as their Monthly Web Tip and was reprinted on our web site with their permission. For additional Monthly Web Tips, go to *www.reid.com* and click on AHelpful Info@.)