MICHIGAN COUNCIL OF PROFESSIONAL INVESTIGATORS

MCPI FALL NEWSLETTER

October 2017

MICHIGAN COUNCIL OF PROFESSIONAL INVESTIGATORS | 37637 Five Mile Rd, #236, Livonia, MI 48154

www.mcpihome.com | www.facebook.com/mcpihome

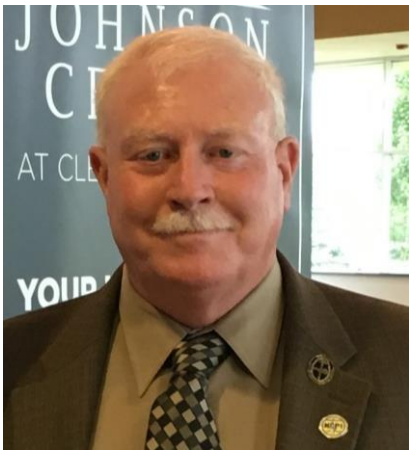
MICHIGAN COUNCIL OF
PROFESSIONAL INVESTIGATORS

***MCPI MISSION STATEMENT**: The Michigan Council of Professional Investigators (MCPI) is an organizational network of investigators from across the State of Michigan founded on integrity, professionalism and high industry standards. Our organization will strive to provide investigators with education, legislative support, business opportunities, and synergistic forums to gather and exchange ideas. The MCPI members maintain the highest standard of ethics and confidentiality to promote trust and support amongst our clients and colleagues.*

In This Issue…

Save the Date!
December 5, 2017
Membership Dinner & Meeting
Novi Oaks Hotel
Register Online!
www.mcpihome.com

President's Message



Dear members,

Thank you to all of the MCPI members and guests who were able to take time away from their business to attend what I believe was a wonderful conference.

Our Fall Conference survey results look very good, and we scored high in all categories. The speakers were well received, and the members who attended tell us the time invested was well worth it. We kicked-off the conference with a full explanation to the new direction your current BOD is taking MCPI and why difficult decisions were made. We are excited and looking forward to creating more value to your membership. There is a lot of work to be done and many members are stepping forward to help as we chart our new course. Membership is growing and people are excited—we will continue our momentum forward to a fantastic 2018!!

To those members not able to attend the Fall Conference, we missed you and look forward to seeing all of you, who are able, at the next membership meeting scheduled for December 5 at the Novi Oaks Hotel and Conference Center in Novi.

Sincerely,

Jerry Hardesty

President, MCPI

GOOD NEWS! MCPI New Website

www.mcpihome.com Click Me!

In June, MCPI launched a new website which brought many improvements to members. The new website tool is also used for:

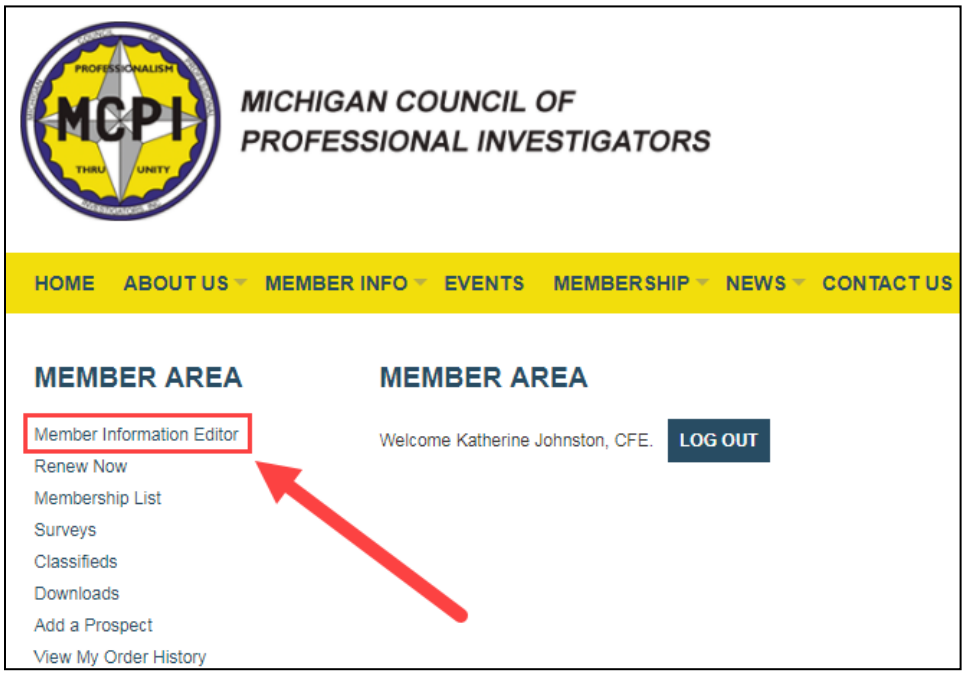
- Maintaining membership data
- Member portal (including ability to edit your profile and listing, view purchase receipts, and utilize Q&A forums)
- Online payment of dues
- Directory of all active MCPI members and PIs
- Online "members only" access to presentation deliverables
- Event registration and management
- Email blasts to all MCPI members
- Announcements and newsletters

It is important that you '*verify*' your email address so that you can be included in mass e-mailings if you haven't already done so. You should have received an email with a link to do the verification and create your login for the website.

Please contact Katherine Johnston (kjohnston@mackinacpartners.com) or Sue Hardesty (sue@hardestyPI.com) if you need additional information or assistance.

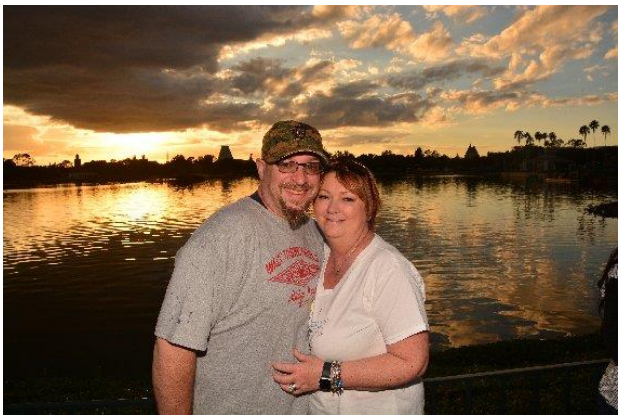
Keep Your Information Updated in the MCPI Database

Using the Member Portal on the MCPI website you can update your contact information, areas of specialty, and choose what information is displayed on the membership list.



Please take a few moments to verify your information is correct.

Featured Sleuth



Jim Schoenherr of Recon Management Group L.L.C. is our current Featured Sleuth and also the current MCPI Sergeant of Arms. Jim was born in Royal Oak and eventually graduated from Utica Ford High School in Sterling Heights, MI. He went to Michigan State University, where in 1993 earned a degree in Criminal Justice and a second degree in Sociology. He had aspirations of moving onto law school, but decided differently after hearing Bill Clinton speak at Michigan State University on the topic of paying students' loan debit if they worked in the Social Services field. Jim worked for seven years with certified emotionally impaired, juvenile delinquents, ages seven to seventeen, at a secured facility called *Children's Home of Detroit* in Warren, Michigan. During this time, he also worked full-time for *J. A. Ditty and Associates* in Troy, Michigan as a Direct Care Staff, Job Coach and House Supervisor, working with adults with closed head injuries and developmental disabilities. For six years, Jim held these two full-time jobs. While working both of these jobs, he hired in at *Recon Management Group L.L.C*. in 1998 as a uniformed, armed security officer. Jim then left the two social service jobs and began working at *Sacred Heart Rehabilitation Center* in Richmond, MI as the Director of Operations working with adults suffering with substance abuse. He stayed there for six months in 1999, leaving in early 2000 when hecame on full-time at *Recon Management Group L.L.C*.

Jim started off as a Field Investigator working surveillance, undercover operations, secret shoppers and jewelry escorts. He worked his way up to Senior Investigator, supervising three other investigators. His next position was Investigation Group Manager, then he became the Director of Security Services. He is currently in charge of all local surveillance, intellectual property investigations, process service and executive protection details, both locally and nationally.

Intellectual Property investigations involve identifying luxury brand purses, hats, shoes, t-shirts, jerseys, etc. Jim is certified as an expert in the Identification of Counterfeit Intellectual Property and he has been invited by various law enforcement agencies to teach Law Enforcement personnel and prosecutors how to investigate and ultimately prosecute the theft of intellectual property with respect to luxury brand items.

On the personal side, Jim has been married for 20 years to Tina, whom he met while working at *J. A. Ditty and Associates*. They worked together for 2 years. Tina is currently employed at *Angel's Place* in Southfield, Michigan. Together they have "three beautiful children"—Eddy, age 36, a full-time shipping and receiving Manager, a former decorated Reserve Officer with Madison Heights and a top 3-Gun competitor in the State of Michigan; Brian, age 33, a stocking employee at a "box store"; and Nicole, age 32, an Arts and Crafts Teacher and mother of four. Jim and Tina have nine grandchildren. They are avid Disney fans and are Disney Vacation Club Members, traveling to the "happiest place in the world" 3-4 times a year. Jim also enjoys the shooting sports, Ford Mustangs and cigars.

Recon Management Group L.L.C. is located at 30400 Telegraph, Suite 472, Bingham Farms, Michigan 48025-2364. Phone: #248-540-0160, Web: www.reconmgmt.com. Jim's E-mail: **jim@reconmgmt.com**. We welcome our New Sergeant of Arms, Jim Schoenherr to the MCPI Board of Directors.

Survey Results for September 19th Training Day

Thank you to everyone who participated in the Training Day held at Cleary University on September 19, 2017. There were 40 MCPI members in attendance and 14 guest attendees. It was a great day.

A survey was sent to meeting attendees and we received 18 responses. The MCPI Board has been reviewing the feedback and will use that information for planning all future events.

Here is a summary of the survey results:

Question	Responses		
Overall, how satisfied were you with the event?	10	55.6%	Extremely Satisfied
	8	44.4%	Satisfied
Was there too much, not enough, or the right **amount of information**?	17	94.4%	Just Right
	1	5.6%	Not Enough
How satisfied were you with the **Venue**?	7	38.9%	Exceeded Expectations
	10	55.6%	Met Expectations
	1	5.6%	Somewhat Met Expectations
Speaker **Scott Bailey** was Informative and Interesting	12	70.6%	Agree Strongly
	5	29.4%	Agree
Speaker **Margaret Scott** was Informative and Interesting	11	64.7%	Agree Strongly
	5	29.4%	Agree
	1	5.9 %	Neutral
Speaker **Stephenie Whitlock** was Informative and Interesting	3	17.7%	Agree Strongly
	5	29.4%	Agree
	9	52.9%	Neutral
Would you **recommend this event** to others?	18	100.0%	Yes

MCPI 2017 Fall Conference Photos

Little Bear with SpyOps sharing equipment & new devices with attendees

Margaret Scott, Attorney & Executive Partner with Secrest Wardle

Presented: Successful Investigations of Insurance Claims

mscott@secrestwardle.com

Stephenie Whitlock, CPA & Kevin Whitlock, CPA

Presented: Best Financial Practices for your Business, Internal Controls and Record Keeping Made Easy

swhitlock@tedderwhitlock.com

Brandy Lord & Candace Ivy with NCISS

Presented*: How the NCISS adds benefit to the MCPI*

www.NCISS.org

Scott Bailey, Partner, *N1Discovery, LLC*

Managing Director of Digital Forensics and Cyber Security, *Mackinac Partners, LLC*

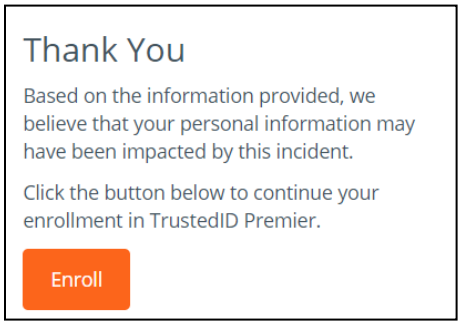
Presented: Ensuring Cyber Security Compliance & Protecting Sensitive Information

Scott.bailey@n1discovery.com

sbailey@mackinacpartners.com

Suggested Approach to Protect your Identity in Light of Equifax Breach…

As you have surely heard, the credit bureau, *Equifax*, was breached, which affected millions of users' data—approximately 143 million as of September 7, 2017. Below are 3 important pieces of info: (1) a link to check to see if your data was breached; (2) the step-by-step instructions for placing a credit FREEZE on your credit with EACH of the 3 credit bureaus; and (3) the top myths about credit freezes. Please note that many sources have recently challenged the accuracy of Equifax's "self-check" tool, thus further convoluting whether or not your data may have been compromised. If you receive the below message, Equifax will try to offer their identity theft monitoring tool—in my opinion, this is a **retroactive** approach (i.e., will alert you *if* something occurs), versus the **proactive** approach of *credit freezing.*



In order to effectively prevent an adversary from opening a line of credit under your identity, you'll need to freeze your credit at each of the 3 credit bureaus. Each of these bureaus now allows the option to apply for a credit freeze directly online. Once your credit is frozen, you will receive a PIN # that can be used (only by you) to temporarily or permanently lift your freeze. *NOTE: you WILL need to temporarily lift your credit freeze before applying for a mortgage, auto loan, etc., OR in most cases, before undergoing a background check. However, the inconvenience a credit freeze poses pales in comparison to the trouble you would face resolving an identity theft crisis.* Please see below for **step-by-step instructions**, as well as the top **myths** about credit freezing:

I. **Check to see if your data was included in the Equifax breach**--
https://trustedidpremier.com/eligibility/eligibility.html (if it was, I'd highly recommend adhering to the below credit freeze steps. I did this it took me all of 10 minutes)

II. Below are the secure websites and processes for credit freezes at each bureau:

a. https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
   i. Enter your personal information (NOTE: this IS a secure website)
   ii. The fees for credit freezes vary by state, but IF you were affected by their breach, you will not be prompted to pay with this bureau.

b. https://www.experian.com/freeze/center.html
   i. Click "Add a security freeze"
   ii. Click "Apply online"
   iii. Enter your personal information (NOTE: this IS a secure website)
   iv. Pay the fee (NOTE: the fee in Michigan is $10, albeit some states are free)

c. https://www.transunion.com/credit-freeze/place-credit-freeze2
   i. NOTE: TransUnion offers both the credit FREEZE and credit LOCK—the freeze is what I am referring to, albeit the above link will first explain the difference between the two
   ii. To freeze, scroll down and click "Initiate Freeze Process" under the sub-section "How do I decide what to do?"
   iii. Same process as above 2 bureaus, although you'll have to create an account first
   iv. Pay the fee

d. Be SURE to retain the receipts and PIN #s for EACH of these transactions (and your username and password for TransUnion)—you'll need these to temporarily or definitively lift the freezes. Although it is surely an inconvenience to have to temporarily lift freezes at times, it is WAY less of an inconvenience than having to deal with the aftermath of identity theft.

III. **Below are some common myths about credit freezing:**

a. "A freeze on my credit will lower my credit score"—***FALSE***! *In fact, with your credit frozen, your credit-related activities will still be reported, thus continue to affect your credit score.*

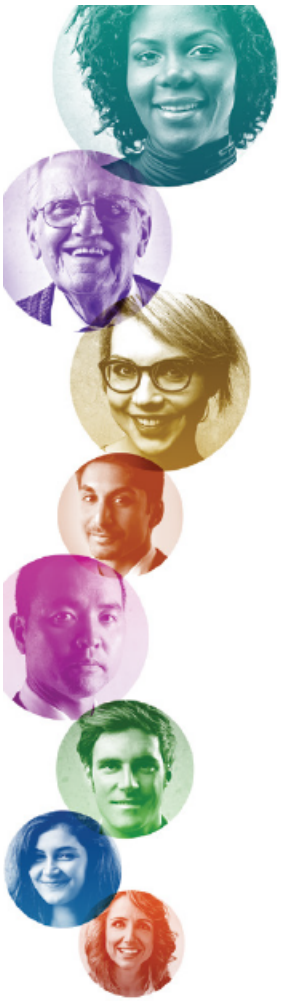
b. "I won't be able to see my credit report without lifting the freeze"—***FALSE***! *You are still entitled to your free annual credit report. Furthermore, your existing creditors can still see your report and score. A credit freeze does not work against companies with which you have an existing relationship.*

c. *"*I froze my credit with 1 bureau, thus don't need to freeze with others."—***FALSE***! *Theoretically the bureaus should communicate, although this is not always the case. The credit bureau you issue a freeze with will not notify the other agencies of the freeze, nor will they be able to extend that freeze to those agencies.*

d. "I won't be able to use my credit cards"—***FALSE***! *You can still use your active credit cards without issue. More so, you can continue to make payments on active loans without issue. These on-time payments will continue to be reported to the credit agencies, thus building your credit.*

For further questions on this matter, please feel free to contact Katherine Johnston, CFE, at kjohnston@mackinacpartners.com

Cyber Security Awareness Month—Homeland Security Tips



CYBERSECURITY WHILE TRAVELING TIP CARD

Cybersecurity should not be limited to the home, office, or classroom. It is important to practice safe online behavior and secure our Internet-enabled mobile devices whenever we travel, as well. The more we travel and access the Internet on the go, the more cyber risks we face. No one is exempt from the threat of cyber crime, at home or on the go, but you can follow these simple tips to stay safe online when traveling.

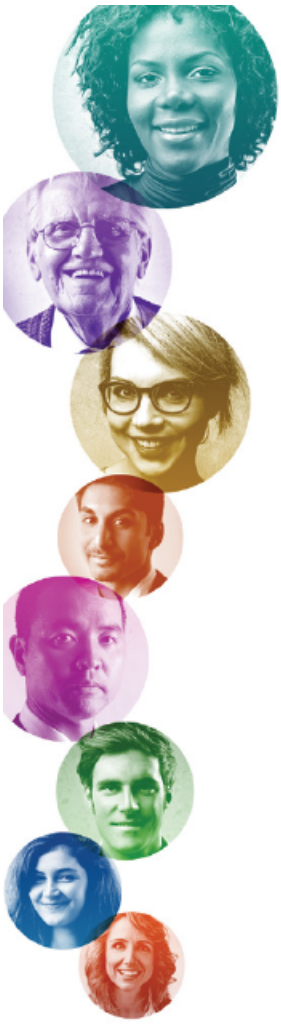
CYBERSECURITY TIPS FOR TRAVELERS

Before You Go

- **Update your mobile software.** Treat your mobile device like your home or work computer. Keep your operating system software and apps updated, which will improve your device's ability to defend against malware.
- **Back up your information.** Back up your contacts, photos, videos and other mobile device data with another device or cloud service.
- **Keep it locked.** Get into the habit of locking your device when you are not using it. Even if you only step away for a few minutes, that is enough time for someone to steal or destroy your information. Use strong PINs and passwords.

While You Are There

- **Stop auto connecting.** Disable remote connectivity and Bluetooth. Some devices will automatically seek and connect to available wireless networks. And Bluetooth enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment systems. Disable these features so that you only connect to wireless and Bluetooth networks when you want to.
- **Think before you connect.** Before you connect to any public wireless hotspot – like on an airplane or in an airport, hotel, train/bus station or café – be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network. Only use sites that begin with "https://" when online shopping or banking. Using your mobile network connection is generally more secure than using a public wireless network.
- **Think before you click.** Use caution when downloading or clicking on any unknown links. Delete emails that are suspicious or are from unknown sources. Review and understand the details of an application before installing.
- **Guard your mobile device.** To prevent theft and unauthorized access or loss of sensitive information, never leave your mobile devices–including any USB or external storage devices–unattended in a public place. Keep your devices secured in taxis, at airports, on airplanes, and in your hotel room.



COMMON CYBERSECURITY THREATS WHILE TRAVELING

- **Unsecured wireless networks.** While public wireless networks provide great convenience, allowing people to connect to the Internet from almost anywhere, they are unsecure and can allow cyber criminals access to your Internet-enabled devices. Beyond the typical public wireless networks found at airports, restaurants, hotels, and cafes, they are increasingly available in other places, such as on airplanes and in public parks.
- **Publicly accessible computers.** Hotel business centers, libraries, and cyber cafes provide computers that anyone can use. However, travelers cannot trust that these computers are secure. They may not be running the latest operating systems or have updated anti-virus software. Cyber criminals may have infected these machines with malicious viruses or install malicious software.
    - One example is keylogger malware which, when installed, captures the key strokes of the computer's users and sending this information to criminals via email. Through this malware, criminals are able to receive users' personal information, such as name, credit card numbers, birthdates, and passwords.
- **Physical theft of devices.** Thieves often target travelers. Meal times are optimum times for thieves to check hotel rooms for unattended laptops. If you are attending a conference or trade show, be especially wary — these venues offer thieves a wider selection of devices that are likely to contain sensitive information, and the conference sessions offer more opportunities for thieves to access guest rooms.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™

Report Suspicious Cyber Incidents

System Failure or Disruption

Has your system or website's availability been disrupted? Are your employees, customers, suppliers, or partners unable to access your system or website? Has your service been denied to its users?

Suspicious Questioning

Are you aware of anyone attempting to gain information in person, by phone, mail, email, etc., regarding the configuration and/or cybersecurity posture of your website, network, software, or hardware?

Unauthorized Access

Are you aware of anyone attempting (either failed or successful) to gain unauthorized access to your system or data?

Unauthorized Changes or Additions

Has anyone made unauthorized changes or additions to your system's hardware, firmware, or software characteristics without your IT department's knowledge, instruction, or consent?

Suspicious Email

Are you aware of anyone in your organization receiving suspicious emails that include unsolicited attachments and/or requests for sensitive personal or organizational information?

Unauthorized Use

Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers, or partners still using your system?

We encourage you to report any activities that you feel meet these criteria. Note that our policy is to keep any information specific to your site and system confidential unless we receive your permission to release that information. US-CERT has partnered with law enforcement agencies such as the U.S. Secret Service and the Federal Bureau of Investigation to investigate cyber incidents and prosecute cyber criminals.

Report an incident to the U.S. Computer Emergency Readiness Team;
Incident Hotline: 1-888-282-0870 / www.US-CERT.gov

For more cyber tips and resources, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign at: www.dhs.gov/stopthinkconnect

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

STOP | THINK | CONNECT™

MCPI Vendor Sponsors

To connect with *EL DORAGO INSURANCE AGENCY*, contact Jesse D. Barber

Cell 313-355-3261; Office 800-221-3386

www.eldoradoinsurance.com

Let's Keep Sailing Forward!