

# The Credit Professional

Fall 2015

Volume 26

## Contents

### **3 Fraud: Reported—Actual— Projected— Prevention/Protection**

*By Linda K. Verges, CFCI*

*Explore the top 10 scams used to bilk consumers out of \$1.7 billion in 2014. Learn how technological advances are making it easier for fraudsters to prey on unsuspecting victims and where the highest risk areas are. Find out what is being done, what needs to be done and what you can do to stop the rampant growth of cyber fraud.*



### **10 Empowering Kansans To Achieve Their Financial Dreams**

*By Lacy Stauffacher and Alicia Marsh*

*Learn how Interfaith Housing Services uses education to help people gain knowledge needed to develop positive financial behaviors, manage their resources and make financial decisions. And find out how the Hutchinson Area Homebuyers Club helps people achieve and sustain homeownership.*

### **14 Integrity—The Consistency of Choices**

*By Warren Martin*

*What is integrity and how do you achieve it? Integrity, the author says, is all about being consistent in making choices about whom you are going to be; your habits; and the opportunities you will face. He offers advice on how to build character through consistency.*

Additional copies of *The Credit Professional* are \$5.00 each for members and \$10.00 each for non-members. To order, contact Credit Education Resources Foundation, P. O. Box 220714, St. Louis, MO 63122. Phone: 314/821-9393. Fax: 314/821-7171. Email: [creditpro@creditprofessionals.org](mailto:creditpro@creditprofessionals.org). Web Site: [www.creditprofessionals.org](http://www.creditprofessionals.org). Payment, by check or PayPal, must accompany order.

## **17 Collections and Social Media**

***By Reagan Merchant***

*Learn how to use social media within collections and continue to protect your clients and yourself. Get the scoop on a recently released handy federal government guide available for your use. And find out what tactics you should avoid using when pursuing collections on social media.*

## **20 Why Should Financial Institutions Consider Lean Six Sigma**

***By S. Michelle Cox, Ph.D.***

*Find out how this process, long used by manufacturing companies, can improve efficiency, effectiveness and communication for firms in the financial industry.*

## **24 Consider the Benefits Of Arbitration in Drafting Your Next Commercial, Consumer or Employment Agreement**

***By Tara LaClair***

*Take a close look at how arbitration can enable you to settle business disputes effectively and efficiently, while saving you time and money.*

## **27 Mergers and Acquisitions: Smooth the Process With Planning and Open Communication**

***By Bruce Werth***

*The key to a successful merger of two companies or organizations hinges on how well and how quickly the newly integrated workforce can embrace the new processes. Based on his personal experiences, the author offers tips on how to make this happen.*

## **30 Tips for Using Public Wi-Fi Networks**

***By The Federal Trade Commission***

*Public Wi-Fi networks are a great convenience but they often are not secure. The FTC offers solid advice on how to protect your privacy when taking advantage of the convenience of these networks.*

# Fraud: Reported—Actual—Projected Prevention/Protection

By Linda K. Verges, CFCI

The Annual Review of the Federal Trade Commission, released on March 6, 2015, reported that consumers lost \$1.7 billion to scams and frauds, according to the reports filed with the FTC in 2014.

The top ten categories of the 2.5 million complaints actually filed are:

**Identity Theft—13 percent.**

Of the 332,646 identity theft complaints filed:

- more than 33 percent were related to Social Security, Medicare and other government benefit programs;
- 17 percent were related to fraudulent use of credit cards;
- 13 percent were related to phone or utilities fraud;
- 8 percent were related to money stolen from bank accounts

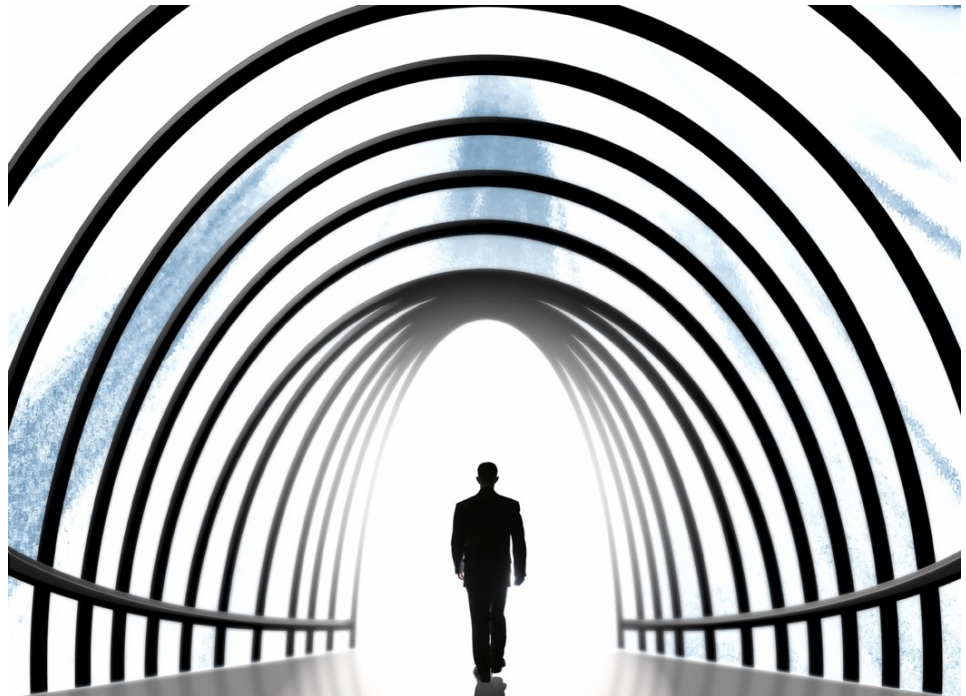
**Debt Collection—11 percent**

- imposters

**Scams—11 percent**

- telephone/mobile

**Services—7 percent**



**Banks and Lenders—5 percent**

**Sweepstakes and Lotteries—4 percent**

**Auto-Related Complaints—3 percent**

**Shop-at-Home/Catalog Sales 3 percent**

**Electronic Media—2 percent**

**Services—2 percent**

The \$1.7 billion in reported losses is approximately \$57 million more than the amount reported in 2013.

Based on the number of complaints filed, the prime target areas or highest risk locales in the United States are Florida, Washington, Oregon, Missouri, Georgia, Nevada, Delaware and Michigan.

*Continued on page 4*

*continued from page 3*

The top three age groups who filed complaints were:

Those in their 50s

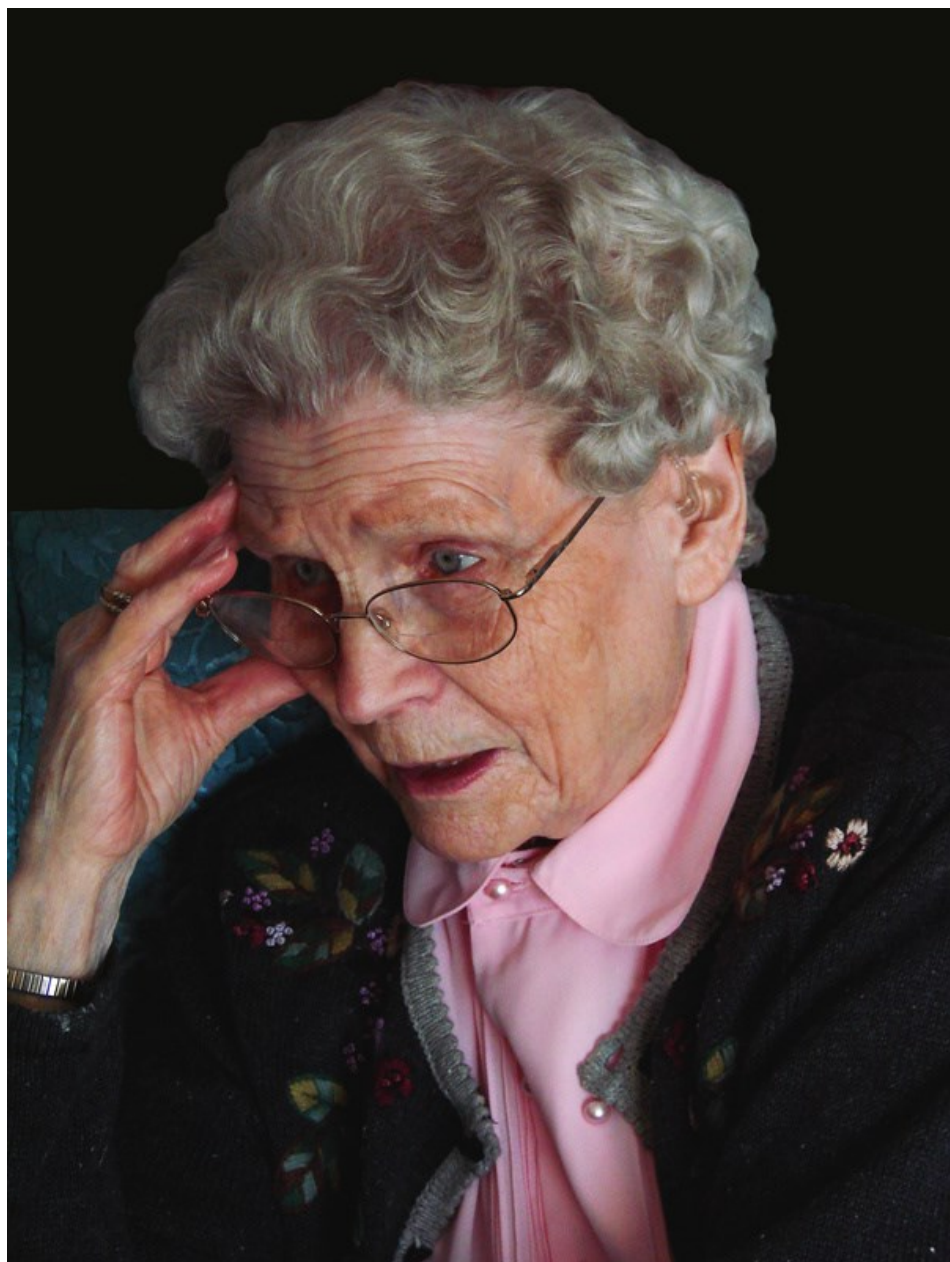
Those in their 40s and 60s

Those aged 70 and older.

The first key in understanding the financial impact of the data disclosed in the FTC report is that it is based on REPORTED COMPLAINTS! The second key is that the report is only those complaints filed by **individuals!** The third key is that the report does not include any information on RECOVERY of losses or PROSECUTION of perpetrators!

In addition, the National Medicare Fraud Task Force estimates that losses to Medicare Fraud are \$60 billion per year, which represents approximately 10 percent of the program's total expenses. Those losses are comprised of 14.5 percent in false home health care company claims; 16.2 percent in fraudulent home hospice service; 33 percent from physicians for unnecessary prescriptions, health services and medical equipment; 28.3 percent for false physical therapy claims; and 8 percent related to kick-backs.

Jennifer Leonard, the FBI agent in charge of the Washington Field Office, has stated: "Fraudsters morph". And the latest reports from one of the national "Fraud Hot Spots" in south Texas indicate that television commercials, telemarketers and door-to-door solicitors have been exploiting new bait-and-switch scams with an all-purpose arthritis kit targeting Medicare recipients.



The products that supposedly provide relief from chronic joint discomfort of knees, backs, ankles, hands and elbows are ineffective braces and wraps, for which Medicare is billed \$3,000 or more as "state-of-art" braces and splints.

The preponderance of daily claims submitted to Medicare is estimated to be an overwhelming \$4.4 million which, by law, must be paid

within 30 days, resulting in the oversight claims review of only three percent or less by Medicare personnel. A U. S. Attorney has referred to these losses as a game of "whack-a-mole".

Medicare fraud could easily increase to 20 or 30 percent of the annual budget due to the number of the qualified aging population and the flexible targeting techniques developed

*continued on page 5*

continued from page 4

by perpetrators. What escapes most of the general public is that the cost of these losses impacts every U. S. taxpayer.

It goes without saying that the consumer-reported and Medicare losses should be considered the tip of the iceberg. Actual **unreported** losses are most likely 25 to 50 percent greater year after year. The long-term impact on the national economy is almost beyond comprehension, with the potential of devastating results.

Technological advances available world-wide have made fraud easier, faster and less accountable than ever imagined by the creators of the internet, software designers and businesses, which have multiplied and which compete to provide customers with quicker, easier, self-fulfilling access to communication, information and products.

With the continuing reports of “hacking” and the vulnerability of the internet, is there anything that can prevent and reduce these economic losses?

According to Eugene Spafford, director of Purdue University’s Center for Education and Research in Information Assurance and Security (CERIAS), the expanding software industry has been built on the premise that flaws can be “patched” and that this “patchability” is a sufficient substitute for sound design.

In Spafford’s opinion, fundamental research is needed to change the way software is

built and deployed. Unless they are changed to a custom-built system, he says, the general purpose, mass-market computing platforms will remain vulnerable to continued cyberattacks. Stafford also notes that, by channeling information to a small number of federal agencies, this centralized, top-down approach handicaps pursuit of malicious cyber activity. Part of Spafford’s solution includes endorsement of a Cybersecurity Czar, combined with local extension services, that would provide education on which software programs do what and how to readily identify problems.

Given that the majority of businesses and individual decision makers are unqualified to select secure software,

Spafford’s proposals have considerable validity. In my limited experience of literally suffering through 10 platform conversions and utilizing one “selective” access platform, I concur with his concept that custom-built software is the only sound approach to cybersecurity. It is expensive but, given the potential losses that can occur using “off-the-shelf” programming, there is no better option.

The recent cases of continuing penetration of U. S. Government data bases clearly indicate that outdated systems, at both state and federal levels, lack the capacity to securely interface with each other. This will only increase the risk of total exploitation of individuals, businesses and



governments. The old adage of “an ounce of prevention is worth a pound of cure” is clearly indicated as requiring immediate attention at all levels.

A second essential component is training and/or educating all users—i.e. employees—of how any business functions, its mission and dependence upon the business’ customers for profitable success and continued employment. Without any doubt, training is an ongoing necessity and, unless employees are selected and indoctrinated with a sound understanding that their work ethic and dedication is vital to the business’ ability to succeed, the result is economic and personal failure. Continuing education, including ethics

that reinforce a firm’s mission statement, membership in professional organizations and acknowledgement of the value of employees’ efforts strengthen the employer/employee relationship.

The importance of this aspect of protection against cyber-crime was evidenced in the penetration of TARGET® in 2014. Prior to that, the Target® operation had been acknowledged as having developed a “state of the art” system to protect its stores.

The corporate offices housed a 24-hour camera surveillance system of all stores and parking lots. The company had two 52-foot self-containing vans with high-tech equipment, which it sent to “hot spots”,

such as Houston and south Los Angeles, where Target’s® CLEET certified personnel join local and sometimes federal law enforcement in sting operations. In addition, each Target® store had CLEET certified personnel, who are expected to protect the facility against shoplifting, dock thefts and related crimes. But Target’s® system had one Achilles heel—human error.

The penetration of Target’s® system was due to the FAILURE of an employee to follow Target’s® standard operating procedure. The perpetrators had done their homework. A bogus representative of the service provider gained access to one of the server rooms at a Target® facility, and the Target® employee who granted entry LEFT the imposter alone in the area—AGAINST STANDARD OPERATING PROCEDURE. The outcome is well known.

Financial institutions in particular—but any well-functioning business—should have in place a precise—and annually reviewed—employee selection process; probationary employment period; consistent initial training program; and a continuing internal training system.

Another aspect of prevention is that all internet users need to be conscious of how to limit their personal and business exposure. As radical as it may seem, it is my opinion that NO EMPLOYEE should ever be allowed to use an employer’s system for personal purposes.



Continued on page 7

Secondly, all individuals can and should take steps to increase their own privacy protection. Specifically, use of the search engines Google, Yahoo and Bing should be avoided due to the tracking each does on the sites visited. DuckDuckGo is a replacement search engine that does not track or market information about users. Digital privacy can also be increased by utilizing encryption programs such as Pretty Good Privacy, Blur or Privacy Badger.

There is usually a minimal cost for encrypting but it can and should be considered money well spent. Finally, dropping the internet and cell phone apps for in-person and snail mail contact should be given serious consideration. More information about digital privacy is offered by the Electronic Frontier Foundation's Surveillance website: <https://ssci.eff.org> and <https://prism-breaking>.

Likewise, businesses, such as banks or credit unions, that have a direct financial responsibility to their employees, customers and clients, should give serious consideration to providing preventive education to each of these groups.

Employee training and tools are vital to the development of consistent and updated loss prevention. Installation of black lights; strict wire transfer confirmation procedures; knowledge of how to detect counterfeit drivers' licenses, checks, debit/credit cards and



money orders; and basic “know your customer” information empowers employees and their employer in frontline fraud prevention.

Additionally, providing customers with information—whether through live seminars or enclosures on statements—not only enhances the customer/business relationship but provides an additional firewall against losses for both.

Examples of fraud prevention information that can be shared with customers include potential losses due to fake Quit Claim Deeds; unpaid property tax scams; overpayment for online items sold; free lunches/dinners to learn how to improve investment returns; lottery prizes; offers to liquidate Time Shares; and the importance of not answering any telephone calls from unknown numbers.

Multiple local, state and federal agencies have online information that can easily be obtained and used to provide detailed educational materials for businesses, employees and customers. These are some of the best resources to protect against fraud and financial crimes. Every state attorney general has a “hot line” for reporting suspicious activity and most county or district attorneys also have fraud, financial crime or white collar crime units, as do city police departments.

These local resources can also provide information on current area or regional scams, fraud and financial crimes. In addition, the FDIC and the OCC have alerts on the internet. A partial list of such resources is included at the end of this article.

Another area of concern is fraud related to ATM and credit cards. In the United States, this

continued from page 7

type of fraud is directly linked to the card issuers—American Express®, Discover®, MasterCard® and Visa®. As early as 2008, these companies were telling U.S. financial institutions that the “chip and pin” system, which activates immediate encryption of transactions and was already in place in Western Europe, would be available in the United States in two years. Those same companies were giving that same two-year

to Europe or beyond must contact their card issuer for a “pin” enhancement that will allow use of their card in other countries. It could be said that the card issuers’ delay is profit driven.

Debit and credit card holders must assume responsibility for monitoring their account activity, as well as bank accounts, especially if engaged in online automatic payments. They must also know the

transfer procedure have been found in the systems of financial institutions. These “bugs” enable the cyber thieves to duplicate the transfer of funds out of the country to their site. As a result of this new development, wire transfer requests and transactions need to be even more closely monitored than before. Taking extra time to confirm wire transfer requests, as well as questioning any “out of the ordinary” amounts or receivers, can prevent considerable losses and strengthen the business/customer relationship.

A good resource to keep abreast of cyber-fraud is Krebs on Security ([krebsonsecurity.livejournal.com](http://krebsonsecurity.livejournal.com)). Many regard it as the fastest and most reliable resource regarding the latest activities challenging businesses and individuals in cyberspace.

In an effort to more efficiently pursue financial crime perpetrators, the FBI recently established a toll free reporting hotline, where analysts collect information from callers and cross check their system for similar reports to enhance investigations and the likelihood of successful prosecution. That number is 855-835-5324.

In addition, consumers can file a complaint with the Federal Trade Commission Bureau of Consumer Protection and/or contact the Consumer Fraud Protection Bureau, the National Insurance Crime Bureau and the FBI.



deadline in 2013. After mid-year 2013, replacement cards with chips began to be issued in the United States but the transition to full utilization of pins was not in place. The card issuers have blamed the financial institutions and retailers for the delay, claiming that they were unwilling to pay the additional cost of upgrading the card scanners and the production of the enhance cards. As of this date, “chip and pin” has yet to be fully activated in the United States. Any American traveling

difference in how disputes of invalid debit card and credit card activity are handled and which party incurs losses.

By now, most financial institutions have put procedures in place regarding wire transfers, to protect customers against scam losses. However, the perpetrators continue to develop ways to penetrate the best-designed procedures.

Recently, previously implanted “bugs” that replicate the wire

Continued on page 9



**Information and Fraud  
Prevention Resources**

**Ethics:**

***Real Rabbits: Chasing an  
Authentic Life***

**Corey A. Ciocchetti (2007)**

**[cciocche@du.edu](mailto:cciocche@du.edu)**

**303-522-7110**

**Professional Organizations:  
Association of Certified  
Fraud Examiners**

**Association of Certified  
Fraud Specialists**

**International Association of  
Financial Crimes Investigators**

**Websites:**

**AARP.org**

**Annualcreditreport.com**

**Donotcall.gov**

**CERIAS.purdue**

**Consumerfinance.gov/contactus**

**Fdic.gov**

**Ftc.gov**

**HHS.gov**

**Kresonsecurity.com**

**NICB.org**

**Act.treas.gov**

**Postalinspectors.uspis.gov**

**Stopmedicarefraud.gov**

**Treasurydirect.gov**

**(additional websites for  
banking commissions, insurance  
commissioners, etc., can be found  
on the internet under  
individual states.)**

About the author:

*Linda K. Verges is a Certified Financial Crimes Investigator who currently contracts as an Independent Consultant. She has over 35 years of experience in finance and banking in Arizona, California, Colorado, Nevada, New Mexico, Oklahoma, Texas and Wyoming.*

*She is a recovery specialist for uninsured losses, repossessions, workout/rewrite loans, fraud, loan and deposit accounts and property valuations. Her experience includes both direct and indirect lending for automobiles, motorcycles, trucks, freightliners, boats, ski-doo's, tractors, manufactured homes, recreational vehicles, commercial properties and undeveloped land. In addition, she has assisted a Chapter 11 Bankruptcy Trustee of a wholesale business in locating and recovering hidden assets and funds.*

*She earned a Bachelor of Arts degree from the University of Oklahoma and received a Master of Arts degree from the University of North Texas. In addition, she has completed over 250 Professional Continuing Education hours related to fraud and financial crimes.*

*Ms. Verges is a member of the International Association of Financial Crimes Investigators and a participant with the Oklahoma City Metropolitan Area Fraud Investigators Association (MAFIA).*

# Empowering Kansans To Achieve Their Financial Dreams

By Lacy Stauffacher and Alicia Marsh

Financial capability cannot be guaranteed by education alone. Long-term, sustainable financial well-being is a dynamic and shifting process that requires a multifaceted approach. Individuals and families are driven by ever-changing life goals and most significantly by their financial goals. Homeownership is one of the most common financial goals households strive to achieve with the highest demand for information and support. Interfaith Housing Services, Inc. (IHS) is working toward meeting these needs for households in the state of Kansas.

The mission of IHS is to develop, promote, and implement programs which assist persons of low to moderate income to meet their housing needs. Since 1992, IHS has helped hundreds of households across Kansas. IHS currently offers a diverse set of services including rental housing, home repair, financial education, and matched-savings programs. IHS is always looking for new ways to help people and has recently expanded its financial education program to include financial capability and first-time homeownership training.



## **Take Control—Grow Your Financial Wellness**

Take Control is a financial wellness program designed for all levels of income to encompass the highest level of individual financial security. Through financial capability training, individuals gain the knowledge to possess positive



financial behaviors, manage their resources, and make financial decisions. Take Control addresses the fundamental components through financial capability training, starting with group education that encompasses goal-and-action-oriented practices. These practices are driven by six behavior principles: visioning, maximizing income, spending, saving, borrowing, and protecting.

### ***Visioning***

Visioning is the process of setting goals, developing a plan to achieve them, and putting the plan into action. This principle is about dreaming big; expressing your heart's desires; building a bridge between

*Continued on page 11*

emotions, thinking, and action; setting goals; giving self-direction; and controlling finances.

**Maximizing Income**

Maximizing income is the process of identifying ways to increase sources of income in order to reach financial goals.



**Spending**

Spending is the process of reducing fees and expenses, as well as, making choices that align with one’s values and goals (both short-term and long-term).

**Saving**

Saving is the process of financially planning ahead. This includes saving for specific financial goals or certain predictable life events and creating a financial buffer for unpredictable financial emergencies.

**Borrowing**

Borrowing is the process of learning other ways to spend money. Special emphasis is given to borrowing via credit. Credit is a tool to get and use something that is paid for later and includes additional costs.

**Protecting**

Protecting is the process of shielding assets from loss due to financial hardships, financial predators and other threats.

Individuals are taught these six behavior principles through hands-on activities, group

discussions and one-on-one financial coaching and support. Financial coaching is offered to all individuals who have attended the group education to further their success of financial security.

Financial coaching is client driven and goal focused. It is centered on performance through practice and accountability. The financial coach offers encouragement and support to practice and adhere to positive financial behaviors. The financial coach will direct the individual with the end in mind and will provide access to a variety of financial products and services to manage their personal finances and reach their financial goals.

**Hutchinson Area Homebuyers Club**

Hutchinson Area Homebuyers Club (HAHBC) is a first-time homebuyer program designed

for all levels of income to achieve and sustain homeownership. Program participants gain awareness of home purchase processes, familiarity with mortgage industry terminology, and understanding of sustainable homeownership practices through homeownership education and counseling services. Homeownership is a symbol of success and gives individuals and families a greater sense of freedom, security, empowerment and independence. HAHBC offers Kansans the opportunity to fulfill their dreams of homeownership.

HAHBC utilizes eHomeAmerica, a nationally recognized and approved online housing education program, to provide the homeownership education curriculum. The online eHomeAmerica Homebuyer Education course covers six topic areas: are you ready to buy a home; managing your money; understanding credit;







## Homeownership Done Right.®

by IHS and has been applied to the practices of both of these new programs. This includes the six core areas of competency—skills training; operational knowledge; code of ethics and conduct; and performance standards. The financial coach and the homeownership counselor have each received training and certification in their respective areas through NeighborWorks America®.

It has been said “knowledge is power”. We believe there is a step missing in this statement—**ACTION!**

Education alone is not going to bridge the gap between information and implementation. Individuals and families in our communities need clear direction and positive support along with accurate information in order to overcome barriers and hardships and to achieve financial goals, whether big or small. IHS is passionate about facilitating success through active programs and is

providing services to meet the needs of Kansas households.

Additional information contact: [aliciam@ihs-housing.org](mailto:aliciam@ihs-housing.org) or [lacys@ihs-housing.org](mailto:lacys@ihs-housing.org)

About the authors:

*Lacy Stauffacher received her bachelor's degree in Communication Science Disorders from Wichita State University. She began working for Interfaith Housing Services, Inc. (IHS), in November of 2013 and took on the role of Financial Capability Coordinator in March of 2015. Prior to this position, she served as the Take Control Coordinator for IHS and facilitated financial wellness classes throughout the Hutchinson area. She has completed the NeighborWorks Center for Homeownership Education and Counseling (NCHCEC) full certification for financial capability, including financial education, financial coaching, and financial skill-building training. She finds satisfaction in delivering accurate information, assisting individuals and families to achieve financial goals, and providing positive one-on-one support.*

*Lacy and her husband live in Hutchinson with their 3-year-old son. She is dedicated to serving her community and enjoys her involvement as an ambassador for the Hutchinson Chamber of Commerce and as a volunteer for Communities That Care.*

*Alicia Marsh received her bachelor's degree in Sociology with a minor in Psychology from MidAmerica Nazarene University where she graduated Summa Cum Laude. She has been working for Interfaith Housing Services, Inc. (IHS), in Hutchinson, Kansas, since November of 2013 and took on the role of Homeownership Coordinator in January of 2015. Since assuming this position, she has completed the NeighborWorks Center for Homeownership Education and Counseling (NCHCEC) training for credit counseling and full certification for homeownership counseling, including pre-purchase and basic foreclosure training. She takes pride in providing guidance and personalized support in all her counseling activities and feels honored to serve her community in this capacity.*

*Alicia and her husband enjoy living and working in Hutchinson. They stay active with their church community, their friends and family, and their 5-year-old puppy—Dakar.*

*Lacy and Alica are new members of CPI. They joined in July 2015.*

**“Without knowledge action is useless and knowledge without action is futile.”**  
Abu Bakr

# Integrity: The Consistency of Choices

**By Warren Martin**

Integrity repeatedly comes up as the number one quality employees are looking for in their boss. This tells us two things:

- 1) the importance of integrity in relationships and
- 2) the fact that there is a lack of integrity in business. If most employers had integrity, it wouldn't be the number one thing employees desired. Although we highly cherish integrity, the reality is very few people can actually define it, which is probably why there is a shortfall.

In hundreds of meetings across the nation, I have asked groups to define integrity. I often get as many answers as there are tables in the room. People will define integrity as being honest, trustworthy, “who you are when no one is looking”, or something along those lines. Most people will define integrity according to a wound they have received. If they have been told a lie, then integrity is someone who is honest. If they have been betrayed, then integrity is someone who is loyal. All of these qualities are important. None of these qualities is integrity.

We live in a world that encourages us to



compartmentalize our lives. When we go to work we put on a persona and at home we put on another persona. We change who we are (how we act, speak and even think) from compartment to compartment. This is seen as normal. It is also why there is little integrity in the world.

To understand integrity, let me take you back to junior high math class—aren't you excited now! In junior high math class you learned a word: integer. Integer comes from the Latin and means “whole”. An integer is any whole number. Integer

is the root word of integrity. Integrity literally means “the state of being a whole number”. Integrity simply means I am a whole person. When you see me at work, then at home, then at church, then at my daughter's basketball game yelling at the referees, if I have integrity, you will see the same person in each case. This is extremely hard to accomplish in a world that encourages you to compartmentalize your life. It is not normal.

Don't ever try to be normal! You will succeed and you will be miserable!

*continued on page 15*

Normal is the average or common type. As we have already seen, the common type is a world lacking integrity. Normality is not a goal—it is the problem!

People of integrity are exceptional. They are individuals who have consistency in their lives. You know what you're going to get when you deal with them. You can trust that what they say to you will be consistent with what they say about you when you're not present. This is why we value them so highly. We know where we stand with them.

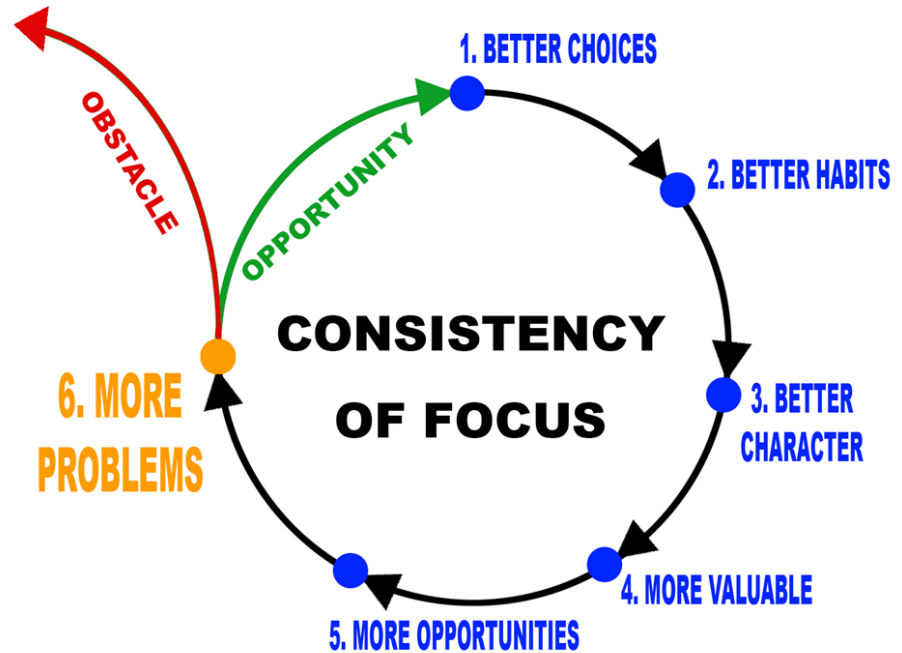
The question is: How do we become people of integrity?

It is all about consistency. It is about being the same person in every situation. This requires deciding who we are going to be. It begins with making better choices on the wheel of consistency.

We get to choose who we are going to be. We do so through the choices we make. We usually want to focus on the major life choices to define our life. Really, it is the endless row of daily choices that define us. That is where consistency is established (or lost).

Better choices lead to better habits. We are creatures of habit. Just about everything we do is based on conditioned habits in our life. From working out, to eating, to reading, to how we get dressed in the morning, literally everything is dictated by habitual actions.

You get to choose your habits. It takes effort and dedication to



© 2000 WARREN MARTIN. ALL RIGHTS RESERVED.

change your habits. You have to consciously choose to initiate a behavior repetitively until it becomes a natural expression.

Better habits lead to better character. Most people have an erroneous view of character. They view character as being trustworthy, responsible, honest, etc. Those are habits. If you are honest, it is because you have the habit of telling the truth. You get to choose your habits but you do not get to choose your character.

Character is how your habits are socially perceived by other people. Better character is achieved when we hold habits long enough that people around us begin to define us by them.

Better character makes us more valuable as individuals and opens the door to greater opportunities. You get to choose the opportunities you will face. Some opportunities take much

longer than others and some take an entire lifetime to develop. However, the opportunities you have today are a direct result of the choices you made, the habits you hold, the character you've developed and the value people place on you. If you want to change the opportunities you get, you have to start by changing the choices you make.

What is the great reward from all this work to become a person of integrity? MORE PROBLEMS—and that is a good thing.

I'm one of the cruelest parents you will ever meet. I do whatever it takes to get my kids out of bed in the morning. I beat pots and pans. I blast opera music through the house. My favorite is to take a mason jar, fill it with glass marbles and put it in the deep freeze.

continued on page 16

If my girls don't get out of bed, I simply pour the jar of marbles into bed with them. You can't roll away from a marble. The only way to get away is to get out of bed.

I will do whatever it takes to get them up, out of the house and down to this little place of torture we call school. While they are there, I insist on a teacher intentionally setting problems in front of them all day. Why? Because I know that, in learning how to solve problems, they become smarter and better.

Isn't it amazing how once we get out of school we think we should have fewer problems? We think if we just make more money or get a promotion we will have fewer problems. The exact opposite is true. We should wake up every morning looking for problems to solve. That is how we become better. It is how we become more successful. Problems are a good thing. They are our opportunity to advance.

Most people's success is defined by how they address their problems. If they talk about and react to their problems as if they are obstacles holding them back, generally, they are

limiting their success. This mentality usually leads to individuals trying to avoid their problems rather than conquering them.

When we begin to see our problems as opportunities, the door is opened to our full potential. Integrity is found when we see our problems as opportunities to make better choices and develop consistency.

Greatness doesn't just happen. It has to be chosen. Integrity has to be chosen. Make a choice and go be great!

*About the author:*

**Warren Martin** is a philosophy graduate of Texas Tech University. He is an author, teacher, minister, artist, quasi-philosopher and speaker known for his unique teaching style. His passion is to inspire and invest in the next generation of leaders.

Warren currently serves as Executive Director of the Kansas Oil Museum, which is dedicated to the preservation and education of the history of Kansas Oil and how it fundamentally shaped the culture and values of America, Kansas and Butler County, especially from World War I to the present, with the goal of inspiring future generations.

He previously served as Executive Director of the General Tommy Franks Leadership

Institute and Museum and was the primary presenter of all Inspired Leadership Experiences.

Warren has been leading leadership workshops, presenting keynote presentations and consulting with Fortune 500 corporations and non-profit organizations for 22 years.

Most recently, Warren has been the subject of a feature article for CPAFocus magazine, a leadership paper published in the Journal of Educational Leadership magazine, and was the recipient of the OKCTEEC Outstanding Community Partner Award and the OK Ethics Community Impact Award (2013 & 2015).

Warren has worked in 28 countries around the world (mostly in the Middle East and Latin America). The author of five books and three articles published by American Association of State and Local History Magazine. He has also worked with teachers, organizations, and youth ministers to develop curriculum and need specific training. Warren has been listed among the top 400 speakers in America. His passion is to invest in the lives of others through servant leadership to assist them in reaching their full potential.

Warren and his wife of 23 years, Wendy, reside in El Dorado, KS. They are the proud parents of four daughters; Bailey, Aisha, Chrysa and Kali. They spend most of their free time spoiling their granddaughter, Tessa.





# Collections & Social Media

by Reagan Merchant, MBA

Collections and how we collect a debt have changed dramatically over the last 10 years. In the collections industry we are accustomed to using skip tracing tools such as LexisNexis, Accurint, and Credit Reporting, as well as calling co-signers and references. We have also added tools to our arsenal over the years—but have you thought to add Social Media?

Social media is everywhere and everyone is using it. It is a part of everyday life. People use it to keep up with trends, find out news and celebrity gossip, to keep up with family and to show others what they have been doing in their lives.

Social media is defined as texting, email, Facebook, Google Plus, MySpace, Twitter, forums, blogs, customer review sites, bulletin boards, Yelp, photo and video sites such as Flickr & YouTube, professional networking, virtual worlds (Second Life). (see page 19, note 1)

According to Facebook's annual report, 95 percent of people who use the internet use social media of some form. Documents, pictures, personal and business info, videos, and music are common things shared. As of December 2014, Facebook had 936 million daily



users, 798 million mobile daily active users on average, 1.44 billion monthly active users, and 1.25 billion mobile monthly active users. (see page 19, note 2)

How does this impact you? Well, financial institutions can use social media in a variety of ways. For example, you can post your new loan promotions, market new products, invite feedback from members, and take payments. You can also use social media to manage vendor relationships; post company updates, new product offerings, acquisitions and employee promotions; follow industry blogs; or keep tabs on trends in the industry.

Interestingly, people are more willing to expose personal details on social media sites than ever before. For example, on March 24, 2015, police in Orange, CT, were able to identify two suspects in a bank robbery, as well as identify their getaway car, after receiving an anonymous tip that led them to several Facebook pages. "This is an example of using good old fashion police work combined with today's social media that led to the successful and quick arrests in this case," said Lt. Andrew Steinbrick. (see page 19, note 3)

A bank robber in Pontiac, Michigan, was identified and located after posting a selfie

Continued on page 18

holding the gun used in the multiple robberies. He was wearing some of the same clothing used in the robbery and was seen on security footage. (see page 19, note 4)

In Houston TX, a man stole a luxury car and then posted the pictures of the keys, as well as his location, on Facebook. Police were able to locate and arrest him on the spot. (see page 19, note 5)

There haven't been any regulations applied to using social media. But, because social media has become a normal outlet, it is now subject to increased scrutiny. There have been instances where collectors used social media and it has resulted in lawsuits. Since then, there are more regulations coming.

The Consumer Financial Protection Bureau (CFPB) and the Federal Financial Institution Examination Council (FFIEC) have released a guide on social media and its use within collections. (see page 19, note 6) This 19-page document outlines the process that was used to determine the guidelines as well as what those guidelines are. This all started in January of 2013, when the FFIEC came up with these guidelines and asked for feedback.

Within this guide is an outline of how to use social media within collections and continue to protect your clients and yourself. Some of these things are skip tracing,



accepting payments, verifying employment and verifying addresses.

Do you use Google Alerts? This is a cool feature and it's free. You set these up so that when the debtor is mentioned on the web somewhere, you'll be notified. These are free and easy to use. They can track keywords, names, company names or executive names. You'll receive an email when the information you entered is mentioned in any story, anywhere.

More and more, courts are allowing Facebook posts to be admissible in court. Since people don't realize there are privacy settings or don't care, they tend to post things that could reflect negatively or be used against them later.

Facebook offers a reverse email search to help you find people. If you don't participate in social media, you should spend some

time learning about them. People, including debtors, spend many hours on these sites and know how to use them. People will post employers, addresses, updated emails, and phone numbers.

Lanie James, with Chesapeake Energy in OKC, spoke to a group of private investigators in OKC recently. She stated that "Many social media outlets now include geo-tracking software that allows members to sign in at different establishments such as bowling alleys, bars and restaurants. Letting friends know where you are via social media sites has become trendy and a lot of establishments offer incentives, including prize drawings, for doing it." She said it becomes so instinctual, such a habit for people to check in, that they don't even think about whether they're where they said they would be or not. People share just so unconsciously." For some people, they see there's a field there and they think they have to fill it in, she said. (see page 19, note 7)

So now that you have an idea of how to use social media, here are some things to avoid:

- posting or commenting on someone's public page about the debtor or their debts;
- sending harassing or threatening messages;
- contacting friends/family;
- posing as a person and friending them on social networking sites.

Neither the FTC nor the FDCPA specifically target social media. There have been talks about

updating guidelines to meet today's standards but, in researching, there wasn't anything more recent than 2009. Mostly this is based on common sense—since there have been recent law suits based on social media and the debtor feeling violated.

Most people haven't read the privacy statements of these media outlets and therefore a lot of pertinent info is left public—such as what they look like; age; date of birth; photos of vehicles; employment info; links to other social media outlets; and status updates that may include when and where they shop, new jobs, major purchases such as homes, and income. This is considered public information and can be used in your collections.

There are major news outlets publishing articles about what collection professionals are doing and how they're doing it, i.e. using social media. Some

people will get smarter about what they post online, while others will continue to think it's just for their "friends".

Anything put out on the internet is there forever, even if deleted.

As a final thought, stay aware of the ever changing landscape and any new regulations.

Consult with your risk assessment person and determine if collecting using social media tools is right for you.

*About the author:*

*Reagan Merchant joined SWBC in April 2007, after graduating from the University of the Incarnate Word (San Antonio TX) with an MBA in International Business.*

*Starting as an Account Manager for the Collateral Protection product, she opted to move to Atlanta GA with the company. Shortly, she returned to San Antonio to pursue a larger*

*territory of South Texas, Oklahoma, and Arkansas, supporting two sales reps.*

*Quickly she started selling additional products and was managing many relationships within the territory. In 2009, she was awarded the Team Player award from SWBC Financial Institutions Group. By 2012, she was on her own in the Oklahoma market. In 2014, she was promoted to Account Vice President within the small to mid-tier sales team. She now covers Texas, Oklahoma, Tennessee & Mississippi.*

*She is a member of Insurance Women of San Antonio. She is currently the President of the OK Credit Union Collections Association based in Oklahoma City.*

Reference notes:

Note 1:  
*as defined by the Consumer Financial Protection Bureau (CFPB)*

Note 2:  
<http://newsroom.fb.com/company-info/>

Note 3:  
<http://www.nhregister.com/general-news/20150324/1-arrested-after-facebook-helps-police-investigate-orange-bank-robbery>

Note 4:  
<http://www.myfoxdetroit.com/story/24923898/facebook-photos-help-police-nab-serial-bank-robbler>

Note 5:  
[http://www.galvnews.com/news/free/article\\_64cec958-cb8a-11e4-95a8-3bae3f6367e9.html](http://www.galvnews.com/news/free/article_64cec958-cb8a-11e4-95a8-3bae3f6367e9.html)

Note 6:  
[http://files.consumerfinance.gov/f/201309\\_cfpb\\_social\\_media\\_guidance.pdf](http://files.consumerfinance.gov/f/201309_cfpb_social_media_guidance.pdf)

Note 7:  
<http://www.pinow.com/articles/344/social-media-expert-offers-skip-tracing-tips-for-private-investgators>

# Why Should Financial Institutions Consider Lean Six Sigma

By S. Michelle Cox, Ph.D.

I am a college professor who teaches classes in TQM/Lean Six Sigma, Change Management, Project Management, and Organizational Learning. I also consult on these things with individual companies that wish to implement or update their continuous improvement programs. However, people still ask me, “Is Six Sigma still around? Do companies actually think it works for them?” Once I stop chuckling at the question, I respond with a resounding, “Yes!” The companies that utilize lean six sigma, and genuinely make the commitment, are able to reduce expenses, shorten cycle times, improve quality, AND meet customer’s specifications.

During the decade of the 1980s, manufacturing utilized lean and six sigma to improve the effectiveness of the assembly line and the efficiency of distribution to customers. In the 1990s, some of these same companies used these methodologies to improve their service organizations. I was blessed to work for General Electric during this time so that I could learn how to use these tools in financial service organizations. Underwriting, product issue, service offices, call centers, eservices, and many other uses became



apparent as companies took huge strides toward building customer centric organizations.

When the methodology for lean six sigma was started, it was MAIC (Measure, Analyze, Improve, and Control). Then, D (Define) was added to the beginning. This first phase is very important to the success of each and every project. Most process owners know the symptoms of the problem, but they have not gotten to the root cause of the problem. At the start of most projects, the problem definition is just a guess. If you solve the problem based on the guess, you are just putting a quick bandage on the problem. But that bandage will come loose and you will

have to work on that same problem again in six months or shorter. However, they do not realize that they are still at the symptom of the problem. Once the problem is defined, that is a working hypothesis that can be accepted, rejected, or updated.

Some companies indicate that they want improvement, however, I am not sure that they all understand how difficult change can be to implement while continuing to run the daily business. The first step in the journey is to find out exactly what your customers want. Financial institutions MUST consider how to improve their processes to continue to build trust and loyalty in their customer base.

When a mistake is made in an account, the customer is unhappy. If it happens again, the customer starts to look for a new provider. Are you keeping track of your mistakes? If so, do you learn from them? In the Define phase, Voice of Customer is one of the most important tools. Once you know what your customer seeks, you can measure to see how well you are meeting their expectations.

The next phase is Measure. When I ask the questions from the previous paragraph of my clients, they usually do not have the numbers. Institutions know how many accounts were opened last year, the profit and loss, the number of employees, and a myriad of other numbers that run a business from an accounting and financial perspective. However, the number of defects in the processes and how these are impacting operations will affect the accounting and financial numbers over time.

Defects are a leading indicator of future losses. The losses are the lagging indicator. When I start with a new client, they usually tell me all about the problems that they are experiencing. In the measure phase, the company works to accept, reject, or update the hypothesis that was built in define. It is only after we start measuring and analyzing the issues that the root cause of the problem becomes apparent.

After we baseline the measure, we start the Analyze phase. There are three or four things, dependent on which expert

is discussing continuous improvement, which can hold the root cause: People, Process, Technology, and/or Communication.

Frequently, companies blame the people for the mistakes. "The people are just here for a paycheck." "These young people do not understand the importance of customer service." Quotes such as these abound.

In reality, it is a tiny percentage of problems that are actually caused by the employees. The employee just happens to be the face of the defect. While many front-line employees have a misguided belief that Lean Six Sigma will result in an elimination of their job, my personal experience of working in the world of financial services, has meant that the employee is recognized for knowing how to solve the problems because they are the people that interact with the customers and know of the

pain points that are experienced by themselves and the customer.

In the Analyze phase, the front-line employee is a key ingredient in the facilitation of an Ishikawa diagram (Cause and Effect Analysis, Fishbone Diagram, Root Cause Analysis). In many projects, the employee participation in the Ishikawa tool starts the change management process in their minds. The employees have become part of building the solution. If the employees feel like a part of the solution, instead of being told they are part of the problem, those employees will adopt and promote the changes necessary for the process and culture change needed for a lasting improvement.

Many managers are concerned about involving the employees in projects and how it will reflect on their ability to lead. I am writing this article to advocate that employee



involvement is the key to understanding your customers. Your front-line employees want their interactions with the customers to be pleasant and add value. By involving them in the root cause analysis, they can share their perspective of interaction with the customer.

We all want to be heard, even if our ideas cannot be adopted. The Lean Six Sigma methodology is important because the use of tools engages your employees in the processes that satisfy your customer. The tools are not something that just checks off a box. The tools are the way to have critical conversations and obtain the data that is needed to solve the problems in a safe environment that does not involve blame. When front-line employees see the open environment, they move from seeing their executives as managers to seeing them as leaders that they are willing to follow based on trust, not just the title.

Once the analysis is complete,

the project moves to the Improve phase. For every Green Belt that I have coached in the last 15 years, this is the point that they sought from the start, and a majority of the Green Belts will readily admit that they would have done different things to “improve” the people, process, technology, and/or communication that would not have been a lasting solution.

In one project, the Green Belt started off with a group of front-line employees who were convinced that their process was as good as it could be because they had spent a lot of time to build it ten years earlier. The Green Belt involved them in each phase. After analysis, one of the employees wrote a two-page email to the executive sponsor telling of the great experience they had through the project tools and how excited they were to be involved. The project involved process changes, new technology implementation, new training for employees, and new communications with the

customer to set expectations. In this instance, all four functions were addressed in the improvement plan. By fixing the process before implementing technology, they did not “make stupid things go faster”, which can happen when the process is not fixed prior to technology implementations.

Once the improvement plan is developed, the Control phase helps the project finalize the following: how the success will be measured, documentation of the process and procedures, execution of the training and communications, and handoff to the process owner from the Green Belt (if the process owner was not the Green Belt). This phase is important because people will continue to do what they will be measured against. The United States is a competitive culture. This competition includes our work habits and how we are measured for development, raises, and bonuses. Many of us even compete with ourselves to be better over time. Tying results to compensation is a part of how companies assure that changes stay in place and that the employees do not revert back to the old, unsuccessful process.

So, do you want to make changes that will engage your employees and delight your customers? Consider using Lean Six Sigma tools and methodology to improve the people, processes, technology, and communications in your company. BUT, do not make this decision lightly. It takes time to implement a program.



For a company just starting the training and projects, you will see your first project completions in one year. It is not a short term fix and thus requires strategic commitment from all levels of the organization. If your organization does not hire certified Black Belts and Master Black Belts into the company, it will take five years to develop them from within. During that time, you will make great strides in solving systemic problems. One of my financial service clients is currently having more than 20 employees trained in Green Belt DMAIC projects (to improve processes), and two employees that are Green Belt certified are now learning

Design for Six Sigma to design new products, processes, technology, and organizations. Each of these individuals is running a project which is solving a problem. They are changing the ways that loans are processed; how customer service addresses phone calls; how work is moved through different departments; and how to remove risk from products and services. Even though it takes time to implement the programs and training, work is being done and large numbers of employees are engaged and the organization is learning!

*About the author:*

*Dr. Michelle Cox has a Ph.D. in Organizational Leadership. She teaches classes to undergraduate and graduate students at The University of the Incarnate Word, located in San Antonio, in the areas of human resources; organizational development; process improvement, change management, project management; and leadership. She also consults for Aventine Hill Partners, Inc., when clients need help with HR, OD, Process Improvement, Change Management and Leadership Coaching. She can be reached via [smcox1@uiwtx.edu](mailto:smcox1@uiwtx.edu) or [michelle.cox@aventinehillinc.com](mailto:michelle.cox@aventinehillinc.com)*

## **Certification—The Key to Your Future**

**Showcases Your Expertise**

**Helps Advance Your Career**

**Recognizes Your Accomplishments**

**Download the certification application form at:**

**[www.creditprofessionals.org](http://www.creditprofessionals.org)**

**The application form is also available by mail from**

**Credit Professionals International,**

**P. O. Box 220714**

**St. Louis MO 63122**

# Consider the Benefits of Arbitration In Drafting Your Next Commercial, Consumer or Employment Agreement

**By Tara LaClair**

In today's competitive and cost-sensitive environment, having the right policies and procedures in place has become more important than ever. This is particularly true with respect to commercial disputes, where litigation costs can quickly escalate and make pursuit of a satisfactory resolution impossible. The good news is there are alternatives to the often long and expensive court system, such as arbitration. The bad news is if you are not currently including arbitration provisions in your contracts, you may not be able to take advantage of this process.



## **What is arbitration?**

It is a streamlined dispute resolution process designed to be an alternative to the court system. It is private and it is contractual. Most disputes can be submitted to arbitration simply by agreement of the parties. It is most common for parties to agree to arbitrate before the need arises but it can also be agreed upon after a dispute occurs. The parties then submit their claims to one or more arbitrators, who make a binding decision.

The decision is final and enforceable. Credit and financial industry leaders will find arbitration provisions can be of use in credit agreements, commercial contracts, certain consumer contracts, and many employment agreements. There are some limitations, however, so talk to an attorney.

## **What are the advantages of the arbitration process?**

Arbitration can have significant advantages over litigating through the judicial system, including the following:

- (1) the parties have more control over the process;
- (2) the costs associated with arbitration are frequently substantially less than those associated with a court proceeding;
- (3) resolution times can be shorter;
- (4) the parties enjoy confidentiality and enhanced privacy; and
- (5) the decision makers, or arbitrators, are selected by the parties and can be chosen based on a variety of factors, such as specific expertise in your business

*continued on page 25*



area. These advantages have made arbitration an increasingly popular means of resolving commercial and consumer disputes, and have resulted in a high level of satisfaction reported by those who have used it.

### **Control over the Process**

Because arbitration is contractual, the parties have significant control over the process from beginning to end. The parties may specify and select the forum for the arbitration, who will serve as arbitrators, and the rules and procedures that will be used for the process, including discovery protocol and the length of the process.

### **Available Forums**

Parties have many options in selecting a forum, including national forums such as the American Arbitration Association (“AAA”), Judicial Arbitration and Mediation Services (“JAMS”) and the National Arbitration Forum (“FORUM”). There are also

industry and smaller regional forums such as the Financial Industry Regulatory Authority (“FINRA”) and the Texas Arbitration and Mediation Services (“TAMS”). These forums have pools of qualified arbitrators and a variety of procedures available for the parties to utilize if they so desire. Most forums allow the parties to completely customize the process to suit their individual needs.

### **Selecting Arbitrators**

In selecting arbitrators to hear the dispute, the parties have many options available. They may select a specific local business person or attorney to serve as the arbitrator in advance, by name. They may select them based on professional experience and background, industry expertise, sensitivity to cost, the number of decisions made or their availability to hear the dispute. Parties may also opt for various list processes used by the different forums. Regardless of which method is used, the parties have control over who

will ultimately hear and decide their case.

### **Procedures and Protocols**

Parties have the ability to customize the procedures that will be used in their arbitration proceeding. Having this flexibility means the parties can design the process to meet their specific needs on a case by case basis. This includes customizing the discovery process, which can mean significant cost savings and shorter time to a resolution. Parties can decide, for example, how many depositions will be taken and where, how long the discovery process may last, how many document requests may be served and what documents and information must be provided as a matter of course.

Discovery is frequently the most expensive aspect of litigation, so having control over these costs can mean the difference between being able to submit a case to the arbitrators for a decision verses settling for less than you believe you are entitled to recover simply because you cannot afford to complete the process.

### **Cost Control**

The primary factors that impact costs are the time it takes to conclude the dispute, the scope of discovery permitted, the extent of the motion practice permitted and the appeal process. In arbitration, each of these factors can be agreed upon by the parties and limited or expanded to meet the unique needs of each dispute. By contrast, parties have little

*continued on page 26*



control over any of these factors in a court proceeding. Instead, the rules of civil procedure apply and allow for broad discovery, depositions of witnesses, extensive production of electronic data and documents, and an extensive motion practice. It can also mean lengthy appeals. This results in average trial costs that could range from \$50,000 to \$250,000, while the costs of arbitrating the same types of disputes could range from \$20,000 to \$150,000.

Costs are also impacted by the length of time it takes to conclude the proceeding. The American Arbitration Association reports the average time to conclude an arbitration matter ranges from four to six months for consumer disputes to eight months for most commercial disputes.

By contrast, Federal district court cases take an average of 23 months to conclude the trial portion and can take up to 40 months to go through an appeal.

### **Privacy and Confidentiality:**

Court proceedings are generally open to the public. Many of the pleadings filed in a court case are available online and can be accessed by the general public. Those pleadings may contain information related to your business as well as the dispute at hand.

By contrast, arbitrations are generally private proceedings and are not open to the public. This means the availability of



the testimony, documents and details of the dispute outside of the arbitration proceeding can be controlled by the parties. Who is permitted to attend the arbitration can also be decided by the parties.

In an era where legal battles could cost your company millions, including an arbitration provision in your agreement can be an effective solution. Studies show that those who have taken advantage of the arbitration process are satisfied with it. These participants sight the expertise of the arbitrators available, the predictability of the outcomes, cost savings and the lack of bias of the arbitrators verses juries as key reasons for their satisfaction.

In addition, studies have shown that there is a high voluntary compliance rate with arbitration awards, meaning the award is more likely to be paid in a timely manner and without additional costs.

In the end, being able to afford to pursue a claim and having confidence that an award will be paid and collected might make the difference in your business model. Consider these benefits when drafting your next commercial, consumer or employment agreement.

### *About the author:*

*Tara A. LaClair is a director at Crowe & Dunlevy and co-chair of the firm's Securities Litigation practice group. She focuses her practice on alternative dispute resolution and commercial litigation. She regularly represents national, regional and local financial institutions, companies and individuals in securities, commercial and employment matters. Ms. LaClair holds a Master of Laws from Georgetown University Law Center; a Juris Doctor from Pepperdine University School of Law; and a Bachelor of Arts in business administration from Eastern Michigan University.*

# Mergers and Acquisitions: Smooth the Process With Planning and Open Communication

**By Bruce Werth**

Throughout my forty-three years of employment, I have been through the merger/acquisition process on three separate occasions. The first was a merger of two groups, with our company being the more dominant of the two, financially and geographically. On the remaining two occasions, I worked for the group being acquired. Interestingly, on all three occasions, the key to a successful reorganization was not a matter of how well the newly-acquired entity dealt with operation integration. Rather, success hinged on how well and how quickly new processes were embraced by the workforce impacted by forced integration.

In today's global market place, mergers and acquisitions are key tools for acquiring technologies and products. They are also a shortcut to improving productivity and profits, honing a competitive advantage, and reducing overall expenses. The success of these "takeovers" is determined by a number of factors, but resistance to them has the potential to negatively



affect the workforce, harm company credibility, and ultimately impact shareholders. These problems can be minimized with careful planning with regard to how staffing, communications, training and customer relationships will be handled once the merger or acquisition takes place.

During any merger or acquisition struggle, there

are at least two groups of employees involved. Often these groups come from distinctly different cultures and uniquely different managerial styles. Certainly, adapting to a new culture is challenging, but this is especially so when uncertainty exists with regard to what the future may hold and whose job may be on the line.

*Continued on page 28*

Research shows that two out of every three mergers are compromised through their failure to consider corporate “culture issues”—i.e. issues that influence a company’s decisions and interactions. Successfully taking on these issues will require companies to reconcile differences, to determine corporate values via a developmental process, and to establish a new identity for the newly-born organization.

To help ensure that the process of a merger/acquisition will be most successful, an employer should:

- Communicate as openly as possible with employees, providing them with a vision and mission for the newly forming organization.
- Inform employees as to what they can expect once the merger/acquisition takes place. This nips inaccurate rumors in the bud and heads off hearsay that can hurt organization morale.
- Preview job expectations for the future combined company. This must be done with staff from **both** groups involved, so all can more realistically cope with any new/modified job demands.
- Handle any layoffs or downsizing as soon as possible to alleviate anxiety, reduce rumors, and return to “business as usual” as quickly as possible.
- Motivate employees during this difficult time by setting aside time to discuss concerns or issues while recognizing the employees openly for their role in managing change.



- Conduct what might be referred to as a “merger/acquisition stress audit” to identify collective concerns of the employees.
- Ascertain the managerial talent required to assure future success of the newly formed company *prior to the merger/acquisition process*. This usually results in top manager turnover no matter how well the process goes.

From my experiences, the success of a merger/acquisition depends on the new company’s ability to help employees envision new cultural perspectives. This is best done via meaningful collaboration between management and employees to define the new culture together. Employee groups encouraged to discover what common beliefs currently exist and what assumptions they share are more likely to see possibilities for the future.

In short, successful mergers/acquisitions are generally the result of reconciled business dilemmas. That means that *everyone* throughout the

newly-formed organization must engage in constructive dialogue if they ever hope to cement their joint goals and strategies into a successful business venture.

*About the author:*

*Bruce Werth was the President of First National Bank in Chicago Heights Illinois for many years and currently is the President of Performance Equity Partners Inc.*

*He is a graduate of the Graduate School of Banking at the University of Wisconsin and the University of Iowa.*

*He is a member of the First Presbyterian Church in Chicago Heights, Illinois, and has served as an Elder and also President of the Session.*

*He was a member of the Kiwanis Club and very active in the community.*

*He has always been very supportive of Credit Professionals International.*



# Credit Education Resources FOUNDATION

## Serving CPI members through:

**Scholarships** for continuing education

**Grants** to support local association consumer credit education programs

**Funds** to publish *The Credit Professional* magazine

**Recognition** of CPI members, via the Helen B. Sawyers HERO Award, for outstanding dedication and achievement to CPI, the credit industry, and consumer education



# AND



## Serving consumers through:

**Sponsorship** of credit education programs for consumers

**Creation** and distribution of *Take Charge of Your Life*, a credit education program created by CPI members for consumers

**Financial** support of the National Center for Missing & Exploited Children, including NetSmartz®, an Internet safety program.

*The Credit Education Resources Foundation is a 501(c)(3) tax-exempt, not-for-profit organization. It raises funds through an annual International Walk-A-Thon and other fundraising events. Donations, which are tax deductible, can be sent to Credit Education Resources Foundation, P. O. Box 220714, St. Louis MO 63122.*

# Tips for Using Public Wi-Fi Networks

## By the Federal Trade Commission

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but often they're not secure. If you connect to a Wi-Fi network, and send information through websites or mobile apps, it might be accessed by someone else.

To protect your information when using wireless hotspots, send information only to sites that are fully encrypted, and avoid using mobile apps that require personal or financial information.



### How Encryption Works

Encryption is the key to keeping your personal information secure online. Encryption scrambles the information you send over the internet into a code so it's not accessible to others. When you're using wireless networks, it's best to send personal information only if it's encrypted — either by an encrypted website or a secure Wi-Fi network.

An encrypted website protects **only** the information you send **to and from that site**. A secure wireless network encrypts **all** the information you send using that network.

### How to Tell if a Website Is Encrypted

If you send email, share digital photos and videos, use social networks, or bank online, you're sending personal information over the internet. The information you share is stored on a server—a powerful computer that collects and delivers content. Many websites, like banking sites, use encryption to protect your information as it travels from your computer to their server.

To determine if a website is encrypted, look for **https** at the start of the web address (the “s” is for secure). Some websites use encryption only on the

sign-in page, but if any part of your session isn't encrypted, your entire account could be vulnerable. Look for **https** on **every** page you visit, not just when you sign in.

### What About Mobile Apps?

Unlike websites, mobile apps don't have a visible indicator like **https**. Researchers have found that many mobile apps don't encrypt information properly, so it's a bad idea to use certain types of mobile apps on unsecured Wi-Fi. If you plan to use a mobile app to conduct sensitive transactions—like filing your taxes, shopping with a credit card, or accessing your bank account—use a secure

*Continued on page 31*



wireless network or your phone's data network (often referred to as 3G or 4G).

If you must use an unsecured wireless network for transactions, use the company's mobile website, where you can check for the **https** at the start of the web address—rather than the company's mobile app.

### **Don't Assume a Wi-Fi Hotspot Is Secure**

Most Wi-Fi hotspots **don't** encrypt the information you send over the internet and **aren't** secure. In fact, if a network doesn't require a WPA or WPA2 password, it's probably not secure.

If you use an unsecured network to log in to an unencrypted site—or a site that uses encryption only on the sign-in page—other users on the network can see what you see and what you send. They could hijack your session and log in as you. New hacking tools—available for free online—make this easy, even for users with limited technical know-how. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs.

An imposter could use your account to impersonate you and scam people in your contact lists. In addition, a hacker could test your username and password to try

to gain access to other websites—including sites that store your financial information.

### **Protect Your Information When Using Public Wi-Fi**

Here's how you can protect your information when using Wi-Fi:

- When using a hotspot, log in or send personal information only to websites you know are fully encrypted. To be secure, your entire visit to each site should be encrypted—from the time you log in to the site until you log out. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Do not use the same password on different websites. It could give someone who gains access to **one** of your accounts access to **many** of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up-to-date.
- Consider changing the settings on your mobile device so it doesn't automatically connect to nearby Wi-Fi. That way, you have more control over when and how your device uses public Wi-Fi.

*Continued on page 32*

- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can get a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees. What's more, VPN options are available for mobile devices; they can encrypt information you send through mobile apps.
- Some Wi-Fi networks use encryption: WEP and WPA are common, but they might not protect you against all hacking programs. WPA2 is the strongest.
- Installing browser add-ons or plug-ins can help. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don't protect you on all websites—look for **https** in the URL to know a site is secure.
- Take steps to secure your home wireless network.

If you don't secure your wireless network, strangers could use it and gain access to your computer—including the personal and financial information you've stored on it. Protect your computer by using WPA encryption.

## Understand How a Wireless Network Works

Going wireless generally requires connecting an internet "access point"—like a cable or DSL modem—to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. Any computer within range with a wireless card can pull the signal from the air and access the internet.

Unless you take certain precautions, anyone nearby with a wireless-ready computer or mobile device can use your network. That means your neighbors—or any hacker nearby—could "piggyback" on your network, or access information on your computer. If an unauthorized person uses your network to commit crime or send spam, the activity could be traced back to your account.

## Use Encryption

Encryption scrambles the information you send over the internet into a code so that it's not accessible to others. Using encryption is the most effective way to secure your network from intruders.

Two main types of encryption are available: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption. WPA2 is strongest; use it if you have a choice. It should protect you against most hackers.

Some older routers use only WEP encryption, which may not protect you from some common

hacking programs. Consider buying a new router with WPA2 capability.

Wireless routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how. If they don't, check the company's website

## Secure Your Computer and Router

- **Use anti-virus and anti-spyware software, and a firewall.** Use the same basic computer security practices that you would for any computer connected to the internet.
- **Change the name of your router from the default.** The name of your router (often called the service set identifier or SSID) is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know.
- **Change your router's pre-set password.** The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. Use passwords that are at least 10 characters long; the longer the password, the tougher it is to crack.
- Visit the company's website to learn how to change the password.