epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

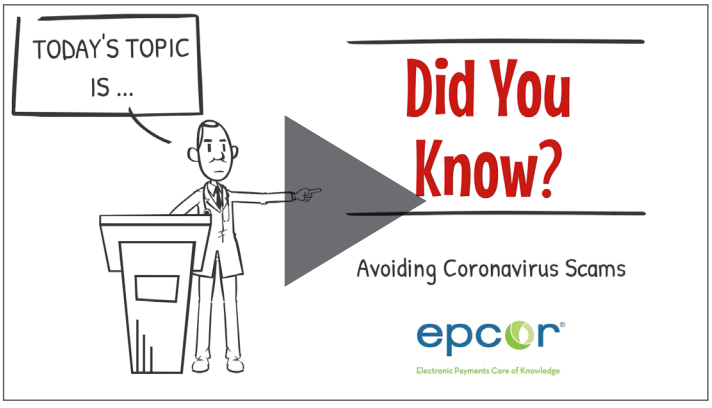
The inside scoop on payments for businesses of all sizes

ACH Rules Update for Corporate Originators

As an Originator of ACH entries, it is important to stay current with the *ACH Rules*, including how updates and changes might impact your business. Differentiating unauthorized ACH Return Reason Codes R10 and R11, a new Same Day ACH processing window and supplementing data security requirements are just a few of the changes on tap for 2020 and beyond. Get up-to-speed on these revisions and how they will affect companies by downloading the ***2020 ACH Rules Update for Corporate Originators***. If you have any questions about how these changes may pertain to your existing Origination activities, contact your financial institution.

Avoiding Coronavirus Scams

Did you know… Fraudsters latch on to any opportunity to defraud consumers and businesses of their hard-earned dollars, and the latest COVID-19 pandemic is their newest tactic? According to a **recent FBI press release**, some red flags to lookout for include unexplained urgency, communications only via email and more. Learn how to identify and combat this new trend by watching EPCOR's new video. You can watch the video at epcor.org/didyouknow or on our YouTube channel. And, for more tips on avoiding scams, check out our BEC scam video (featured on page 5).



5 Tips for Business Professionals Working from Home

by Natalie Bartholomew, Grand Savings Bank, Author of The Girl Banker

We are in uncharted territory, friends. Unfortunately, no one wrote a book on how to handle the situations we are currently facing. If you or your employees are working

remotely during these unprecedented times, here are some tips that might help you in this new environment.

1. Pretend You're Going to Work as Usual

Let's be honest, dressing comfortably and

see HOME on page 2

HOME continued from page 1

opting out of "getting ready" as you typically would for a day at the office is going to happen! However, there is something to be said for keeping your morning routine as close to normal as possible. Ann Buckmiller, Compliance Officer of Reliabank in Watertown, SD says, "Getting ready in the morning is HUGE for me. It really helps with productivity and sticking with my work routine. Set your alarm, exercise, take a shower and get to work." Tim Martinson, Marketing Manager at North American Banking Company in Roseville, MN, suggests keeping the same hours as you would at the bank. "There is a temptation to start work early, work late, etc. Staying on the schedule helps with work/life balance, which applies to those working at home."

2. Set Up a Separate Workspace

I've tried camping out on my couch with my laptop, planner and phone and trust me, it doesn't exactly set you up for a day of productivity. Instead, Sam Burrington, AVP Digital Project Manager at Morgan Stanley and former community banker suggests setting up a separate workspace in your home and bringing all of your "work essentials" to that space such as your laptop, charger, coffee, planner, etc. "If you don't have a home office, set up a folding table. I sit at my dining room table when the kids are playing and when I'm not hosting calls. If I need to jump on a conference call, I go to my dedicated space."

3. Stay Social

FOMO (fear of missing out) when working from home is real! And, you may worry that you are missing out on all the important conversations or happenings "around the office." You may also feel that others don't think you're working hard because they can't physically see you working. Burrington goes on to stress the importance of over-communicating with coworkers. "Pick up the phone instead of sending an email. Try to have quick 'how are you doing' conversations to emulate in-person exchanges."

4. Establish Boundaries with Your Family and for Yourself

You may be looking forward to "quiet" time at home to focus on work with little interruption. And then you find yourself distracted by the need to tackle the growing pile of laundry or feel guilty for not hanging with the kids. Establishing boundaries with your partner and kids can set the tone that you have work to do and they can reach you via text or cell just like they would when you're in the office. Otherwise, you might find you will get interrupted frequently as you do at work! "Set an alarm to get up and stretch, grab more coffee, take a lunch break and walk around just like you would at the office," said Martinson. Additionally, Autumn Albright, Marketing and Sales Coordinator at Civista Bank in Sandusky, Ohio, suggests coming up with planned activities or a schedule for your kids if they are at home with you. This helps with keeping them busy during the day while you're working.

5. Give Yourself a Break

This tip may apply a little more toward current circumstances than any other time one may work from home, but we all need to remember that none of us have all the answers on how to handle this pandemic perfectly. As I'm typing this, I am looking around my house and it looks like a bomb went off. I've only been home two days and I've yelled at my kids, worked too much, stayed up too late, skipped lunch and drank way too much wine. It's a stressful, uncertain time. My family has been more than understanding and it's helped to have financial professional peers to reach out to for guidance and advice. Remember that we are all in this together and this too, shall pass.

Source: The Girl Banker

Is YOUR Business Prepared for an Emergency?

by Karen Nearing, AAP, APRP, CAMS, CRCM, NCP, Director, Regulatory Compliance Education

The recent COVID-19 pandemic has shed new light on business continuity planning, forcing businesses everywhere to come to terms with their planning efforts.

A Business Continuity Plan (BCP) is a plan to ensure that business processes continue during a time of emergency or disaster. Normally when we think of a disaster or emergency, we think weather-related. However, recent events have shown us that emergencies can come in unusual forms and no business is immune. While the adjustments your company has made to adapt to some of the restrictions placed to flatten the COVID-19 curve are fresh in mind, it is an ideal time to look at your BCP to ensure it is up to date and you are prepared the next time an emergency impacts your business.

Your company's BCP should:

1. Identify the scope of the plan
2. Identify key business areas
3. Identify critical functions
4. Identify critical resources
5. Identify dependencies between the various business areas and functions
6. Determine acceptable downtime for each critical function
7. Create a plan to maintain operations

After the plan has been created, there should be testing of the plan to include:

1. Table-top exercise
2. Structured walk-through
3. Disaster simulation testing

see EMERGENCY on page 6

Bad Checks, Bad Checks – Whatcha Gonna Do?!

by Marcy Cauthon, AAP, APRP, NCP, Director, On-Demand Education

Does your business still accept paper checks for payment? If you answered yes, you're not alone. Some businesses still have a lot to gain by accepting checks for payment. For example, certain businesses don't accept debit or credit cards because of processing fees, and checks can be a great alternative.

The challenge businesses face when accepting check payments is knowing how to avoid bad checks. You never know for sure if clients have money in their checking accounts, and it is expensive and time-consuming when checks bounce as financial institutions charge businesses bad-check fees. As a business, you have the time and costs of check collections to consider as well.

Here are some tips according to *The Balance* to reduce the odds of taking a bad check:

1. If your business accepts checks, have an iron-clad check cashing policy. Verify the payee's identification before accepting a check. Ensure the payee endorses the check in your presence.
2. Ensure that the client's contact information is printed on the check. If it's not, or it's not up to date, request a current address and telephone number. If something goes wrong with the payment or the check collection process, the first step is to contact the client and let them know, so valid contact information is essential.
3. Inspect the check to determine whether it was printed by a professional check printer or was potentially created by a professional thief. Look to see if the edges are cleanly cut and square, and look for security features on the check, such as watermarks or microprinted words that are so small that they are barely distinguishable to the naked eye.
4. Look for any signs of tampering, including crossed-out or rewritten marks, handwritten letters or numbers outside of the fillable lines, different ink or smudging as this could indicate an alteration.
5. Review the amounts written on a check. Amounts should appear twice on each check. Written out in words and written numerically. If a discrepancy arises between the two, a financial institution will honor the written amount.
6. Watch out for low-numbered checks. Usually, a low number means a new account, perhaps one that was set up to defraud a business. The odds are increased that these low-numbered or starter checks are fraudulent. Of course, a low-numbered check is not inherently bad—we all had to start our checking accounts sometime. But statistically, the incidence of fraudulent checks rises with low check numbers.
7. Scrutinize every check. Look for inconsistencies and things that just don't seem right. For example, personal checks with four smooth edges (no perforations) or shiny print jobs are worth a second look. They may be counterfeit checks produced on a laser printer. Also, compare the series of numbers at the top and bottom of the check: The last three or four numbers of the Federal Reserve number at the top of the check (usually at the upper right) should match the first three or four numbers of the routing/transit number (usually on the lower left).
8. Don't spend deposited checks right away. Remember that a check can be returned and charged back against your account. This process might take longer than you expect, as fraudulent items may not be discovered until an account holder receives their statement.
9. Review your business account activity online daily. This helps to determine if counterfeit checks have hit your account. Catching counterfeit checks timely is crucial, as your financial institution only has 24 hours to get the check returned.
10. Try taking local checks only. Out-of-state checks are at a higher risk to be fraudulent. This may not always be ideal, so if you take out-of-state checks, ensure you have a policy of how these items will be handled.

Source: TheBalance.com

Why is My Financial Institution Asking for More Stuff?

by Jennifer Kline, AAP, APRP, NCP, Director, Audit Services

Your company may process payroll or vendor ACH payments. Or, you might capture check images through your institution's business online banking product, or collect payment from clients for the goods and services you provide to them. Whatever your use-case for processing ACH and check transactions might be, the *ACH Rules* (such as the updates mentioned in the *ACH Rules Update for Corporate Originators* on page 1) and other regulatory requirements impact you as an Originator, too. Your financial institution makes legal warranties on your behalf to other businesses that you will comply with the *Rules* and U.S. laws; therefore, you also bear some of that responsibility. Let's talk about what your financial institution might look for or ask you to provide to ensure you are in compliance with applicable rules and regulations.

One such responsibility relates to how you secure banking information. To ensure you understand your responsibility, your financial institution may be asking for more information about your business practices. They may be asking questions such as:

- How are you keeping banking information secure, both in paper and electronic formats?
- How long do you retain banking information?
- What method do you use to destroy banking information after you are no longer required to retain it?
- Do you keep paper authorizations and checks in a locked fireproof cabinet? If so, who has keys to the cabinet? And, can anyone get access into the cabinet?
- Are your internal computers and network secured with unique user IDs and encrypted password security?
- Are there employee controls over who has access to certain files, encrypted data or sensitive data, such as payroll?

While these questions may seem intrusive, they are asked to ensure you are taking measures to protect sensitive banking information and maintain the integrity of transactional data.

In addition to data security, you also have a responsibility to ensure physical controls at your company are functioning properly to reduce risk. Your financial institution may ask you questions such as:

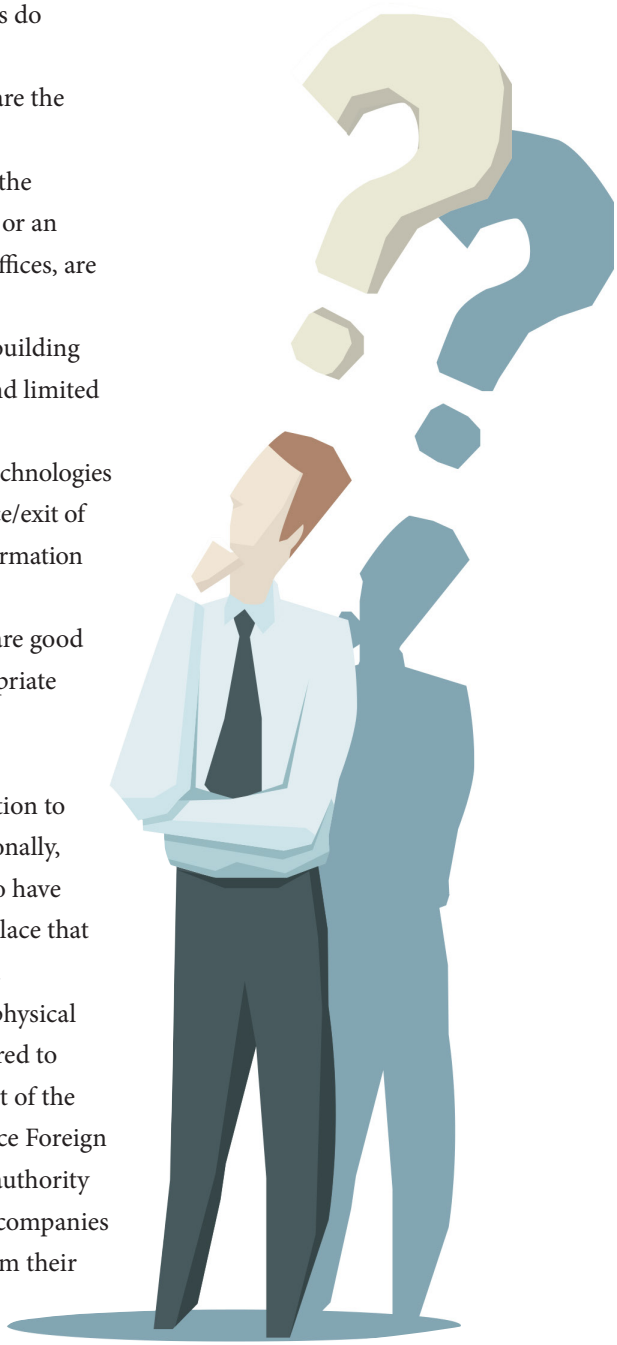
- How many physical locations do you have?
- Can anyone enter offices or are the doors locked and restricted?
- When a third-party, such as the cleaning crew, an electrician or an auditor is in the backroom offices, are they required to sign in?
- Can third-parties roam the building freely or are they escorted and limited to specific areas?
- Are there cameras or other technologies in place to record the entrance/exit of people from areas where information and systems are stored?

These physical security controls are good ways to manage the risk of inappropriate access to information and systems. Typically, these controls are also established at your financial institution to protect your company data. Additionally, financial institutions are required to have vendor management programs in place that function effectively to mitigate risk.

In addition to data security and physical controls, Originators are also required to follow all U.S. laws. As a component of the U.S. Treasury Department, the Office Foreign Assets Control (OFAC) derives its authority from a variety of U.S. laws. Payroll companies may get the following questions from their financial institutions:

- What steps are you taking to examine employees through OFAC?
- Do you periodically review the Specially Designated Nationals (SDN) list?
- What do you document when you investigate new employees?
- Have you verified each employee before you send payroll out through the ACH Network?

see STUFF on page 7



Third-Party Senders with Third-Party Senders as Clients… Say What?

by Karen Nearing, AAP, APRP, CAMS, CRCM, NCP, Director, Regulatory Compliance Education

News media erupted in September 2019 with stories of innocent employees who not only had their payroll reversed but had also suffered from an additional reversal. Upon further investigation, MyPayrollHR (a Third-Party Sender) was linked to the processing of these payments and subsequent reversals. A few weeks later, another Third-Party Sender, Cachet, found itself in the spotlight for not processing files created on behalf of its clients. MyPayrollHR and Cachet had worked together with some processing of transactions and the failure of one led to issues with the other. In light of these recent events with Third-Party Senders who had Third-Party Senders as clients, also referred to as "nested" Third-Party Senders, it is a good time to analyze your payment processing procedures if you are using an external firm.

As the industry continues to push to make payments faster and all electronic, many businesses have outsourced accounting services because they do not have the manpower or experience to streamline processes to pay accounts payables, collect receivables and process payroll. One of the ways a business might do this is through services provided by another company, a service provider. While there is not a one-size-fits-all approach to offering these services, many times the service provider is granted access to the business' online banking/cash management services to create transactions. However, other times the service provider uses its own platform and financial institution to process these transactions, which makes the service provider a Third-Party Sender. And, to make things more complicated, that Third-Party Sender may use another service provider to get the transactions into the ACH Network, which then leads us to a Third-Party Sender with a Third-Party Sender as a client.

Is your company involved in any of these relationships?

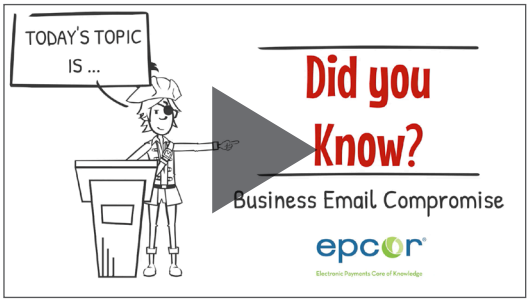
The first question to ask is… do we have any Third-Party Senders? A Third-Party Sender is defined in the 2020 *ACH Rules* on page OR68 as "a type of Third-Party Service Provider that acts as an intermediary in transmitting entries between an Originator and an ODFI, including direct access, and acts on behalf of an Originator or another Third-Party Sender."

You might be wondering; how do you know when Third-party Senders have Third-Party Senders as clients? As part of your due diligence on any vendor agreement, your company should understand the service provider's business, who they are serving and in what capacity they are serving. As an Originator, you are ultimately responsible for every transaction your service provider transmits through the ACH Network on your behalf. Having substantial vendor management in place is key to knowing how your payments will be processed.

Any relationship has its risks, it is up to your company to understand how the different parties fit together, keep track of who is responsible for what and know the financial standings of your service provide. Your reputation and your business depend on it!

Be Aware of Business Email Compromise

Did you know… The FBI released a public service announcement that business email compromise (BEC) scams are on the rise? The scams are continuing to evolve, targeting small, medium and large businesses as well as personal accounts—reported in all 50 states and 150 countries. In this time of uncertainty and many people working remotely, learn how to spot possible scams and tips for combating the fraudsters. You can watch the video at epcor.org/didyouknow or on our YouTube channel.



Have You Gone Above and Beyond in this Time of Need?

STELLAR SERVICE?

INNOVATIVE PRODUCTS?

COMMUNITY OUTREACH?

Your efforts deserve to be recognized! Apply for an EPCOR Payment Systems Award, presented at EPCOR Payments Conferences, at epcor.org.

You Can Still Level-Up Your Payments Career this Year!

If you are thinking of achieving a payments accreditation in 2020, you can still work toward your goal! Nacha and ECCHO have moved exam windows to the fall in light of travel restrictions.

To find out more about becoming an AAP, APRP or NCP with help from EPCOR's *Prep Programs* visit epcor.org.

The Federal Reserve Releases Payments Study

The 2019 Federal Reserve Payments Study is the seventh in a series of triennial studies conducted by the Federal Reserve System since 2001. The goal of this study is to estimate aggregate trends in non-cash payments in the United States. Your company may want to review the study's results to help determine how consumers are paying today and review different payment options available to you at your financial institution.

The study found accelerating growth overall in core non-cash payments (ACH, cards, checks) from 2015 to 2018 compared to the previous three-years.

The study also found that:

- Debit and credit card payments grew 8.9% per year between 2015 and 2018.
- The value of remote general-purpose card payments in 2018 nearly equaled that of in-person payments.
- More than half of in-person general-purpose card payments were chip authenticated in 2018, up from 2% in 2015.
- ACH payments grew 6% per year between 2015 and 2018.
- Check payments fell 7.2% per year from 2015 to 2018.

To view the full study, **click here**.

Source: Board of Governors of the Federal Reserve System

EMERGENCY continued from page 2

A review of your plan should be held periodically to help improve the plan, as well as raise awareness of what the plan states. Everyone in the organization should be included and aware of the BCP so that they can assist in the event key personnel are not able to complete the plan's assigned duties or tasks.

One of the best ways to ensure your BCP will work appropriately is to look at your processing procedures. Think about how systems run or can be modified to ensure your organization can continue to support your clients and employees if the normal daily processes are interrupted due to lack of staff or a natural disaster. To some extent, you can test your institution's BCP during events such as natural disasters, but the loss of key personnel could be greater in a pandemic and inhibit the expected knowledge base available to maintain the plan. The ability to work remotely or through a flexible work environment should be a consideration should personnel be confined to their homes due to quarantine.

Having updated policies and procedures that are easy for everyone to understand and follow, even if the duties and tasks fall outside their normal scope of work, is vital for your organization.

Now is the time to prepare so you have a plan in the event of the next emergency. Create a plan, test the plan, update the plan, test the plan, update the plan... is the best cycle to be in so you are ready for an emergency situation.

Explore EPCOR Membership

If you would like more payments-related guidance, resources and information to help you through the COVID-19 pandemic or any other payments challenges, consider becoming an EPCOR member.

Explore your options by calling 800.500.0100 or visiting epcor.org.

STUFF continued from page 4

Financial institutions have controls in place to check their client database against the OFAC list on a daily, weekly or monthly basis; however, under U.S. law you must also take steps to ensure your compliance.

This is not a complete list of the questions you may be asked by your financial institution. And, while all these additional questions may be exasperating, remember that adhering to rules and regulations helps protect your company from both legal, monetary and reputational risks. It is in the best interest of you and your financial institution to do periodic checks to make sure that you are protecting yourself and your company's clients. Keeping proper documentation, storing information securely and adhering to time restrictions and other requirements are part of your obligations. If you are unsure whether the controls you have in place will result in compliance with rules and regulations, you should reach out to your financial institution for assistance.

In addition to working with your financial institution, you can also partner with a compliance expert to evaluate the risk. EPCOR's advisory and audit staff members are ready to help your organization identify weaknesses, mitigate risk and improve your profit margin. If you are interested in having a fresh set of eyes review your organization's processes, practices, policies and procedures, contact our team at audit@epcor.org or advisoryservices@epcor.org.

So... Are You Required to Provide That?

As an Originator or Third-Party Sender, there may be times your financial institution requests documentation from you. There are also key retention periods required within the *ACH Rules* that must be followed. The following table will help you comply with your *ACH Rules* obligations:

FROM	TO	DOCUMENTATION/RETENTION PERIOD	TIMEFRAME TO PROVIDE
Originator (Your Company)	Your Financial Institution	At the request of your financial institution, you **must** provide the original, copy or another accurate record of the consumer's **authorization**.	Provide in such time and manner as to enable your financial institution to deliver the authorization to the requesting institution **within ten Banking Days** of the institution's request. The financial institution may have shorter timeframes they request these items from you to ensure the *Rules* deadline is met.
		At the request of your financial institution, you **must** provide for a CCD, CTX or Inbound IAT entry to a non-consumer account either (1) an accurate record evidencing the Receiver's (i.e., trading partner's) **authorization, or** (2) **contact information** for your company that, at a minimum, includes (i) the company's name, and (ii) phone number or email address for inquiries regarding authorizations of entries.	Provide the record or information to your financial institution for its use or for the use of the requesting institution in such time and manner as to enable your institution to deliver the information to the requesting institution **within ten Banking Days** of their request.
		Your company will securely store and retain a reproducible and legible copy of the front of the Receiver's **check used to initiate an ARC or BOC entry** for two years from Settlement Date of the ARC or BOC Entry.	Provide copy to your financial institution upon request as to enable them to deliver to the requesting institution **within ten Banking Days** upon receiving their written request. The requesting institution's request must be received within two years of the ARC or BOC Entry Settlement Date.
		Your company must retain a copy of the front and back of the check to which an **RCK Entry** relates.	Provide copy to your financial institution upon request as to enable them to deliver it to the requesting institution **within ten Banking Days** of receipt of their request.
Third-Party Sender	Your Financial Institution	Must retain proof/documentation that you have completed an **annual audit** in accordance with the *ACH Rules* for a period of six years from the date of the audit.	Provide in such time and manner as to enable your financial institution to deliver proof to Nacha **within ten Banking Days** upon Nacha's request.
		A Third-Party Sender must, upon its financial institution's request, provide them with any information they reasonably deem necessary to **identify each Originator** (i.e., client/customer) or other Third-Party Sender for which they transmit entries.	Provide **within two Banking Days** of receipt of your financial institution's request.
		A Third-Party Sender must provide its financial institution with the information required by Subsection 2.17.3 (**Third-Party Sender Registration**) for purposes of their registration of your company with the National Association (Nacha).	Provide **within two Banking Days** of receipt of your financial institution's request.

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit trade association devoted to providing timely and relevant payments education and support to our members to help them maintain compliance, improve operational processes, and mitigate risk and fraud. Through our affiliation with Nacha and other industry associations EPCOR fosters and promotes improvement of the payment systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha™ Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
3100 Broadway Blvd., Ste. 555, Kansas City, MO 64111
800.500.0100 | 816.474.5630 | fax: 816.471.7665