epcor®
Electronic Payments Core of Knowledge

INSIDE ORIGINATION

Have You Familiarized Yourself With the 2017 *ACH Rules* Changes?

As an Originator of ACH entries it is important for you to stay up-to-date with the *ACH Rules*. Same Day ACH debits became a reality on September 15, and the Third-Party Sender Registration Rule went into effect September 29. Do you know how these changes might impact your business and/or your relationship with your financial institution? Or do you still have questions on just what the changes might mean to your organization?

Download the ***2017 ACH Rules Update for Originating Companies*** to discover answers to your important questions. For further details on how these changes may pertain to your specific Origination activities, contact your financial institution.

Are you a Third-Party Sender?

If your financial institutions suddenly asks questions about your business, don't be alarmed! They are gathering information to provide to NACHA to comply with the new Third-Party Sender Registration Rule. To acknowledge the importance of these players in the ACH Network, NACHA has launched their Third-Party Sender Certification Program. You can become NACHA Certified when they have met NACHA requirements for employing effective oversight of your business, understanding ACH risk and compliance obligations, and demonstrating sound governance. Get more information in the article on **page 3** and from **NACHA's website**.

Protect Your Business Against Wire Transfer Fraud

An old scam with the potential to impact the bottom line has resurfaced: wire transfer fraud. Fraudsters target businesses through email phishing scams by impersonating a business executive, partner or trusted vendor.

In this scam, fraudsters target companies most likely to make wire transfers. Typically, the criminal gains access to the legitimate

see FRAUD on page 3

10 Cybersecurity Tips for Small Businesses

Broadband and information technology are powerful tools for small businesses to reach new markets and increase sales and productivity. However, cybersecurity threats are real and businesses must implement the best tools and tactics to protect themselves, their customers and their data. Visit **www.fcc.gov/cyberplanner** to create a free customized Cybersecurity Planning guide for your small business and visit **www.dhs.gov/stopthinkconnect** to download resources on cybersecurity awareness for your business. Here are ten key cybersecurity tips to protect your small business:

1. **Train employees in security principles.** Establish basic security practices and policies for employees, such as requiring strong passwords and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

see TIPS on page 2

TIPS continued from page 1

2. **Protect information**, computers and networks from cyber attacks. Keep clean machines: having the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.
3. **Provide firewall security** for your Internet connection. A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.
4. **Create a mobile device action plan.** Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.
5. **Make backup copies** of important business data and information. Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.
6. **Control physical access** to your computers and create user accounts for each employee. Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.
7. **Secure your Wi-Fi networks.** If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

8. **Employ best practices** on payment cards. Work with financial institutions or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your financial institution or processor. Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the Internet.
9. **Limit employee access** to data and information, and limit authority to install software. Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.
10. **Passwords and authentication.** Require employees to use unique passwords and change passwords every three months. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

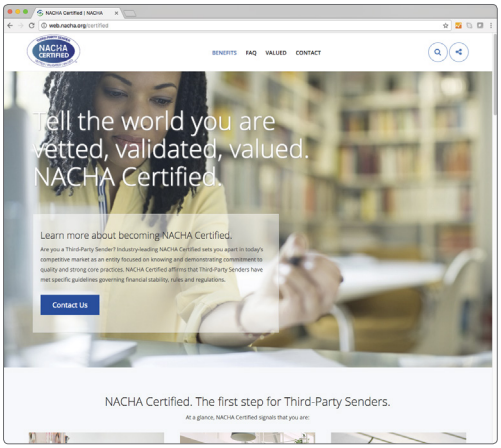
Source: Federal Communications Commission

NACHA Launches Third-Party Sender Certification Program

In April, NACHA launched a new certification program for Third-Party Senders called NACHA Certified.

Third-Party Sender organizations can now become NACHA Certified when they have met NACHA requirements for having employed effective oversight over their business, understand ACH transactions processing risk and compliance obligations and demonstrate sound governance.

"Third-Party Senders are important and valued players in the ACH Network, and help businesses and other organizations benefit from originating ACH payments for services," said NACHA President and CEO Janet O. Estep. "NACHA Certified organizations demonstrate that they are vetted and validated with sound core practices in place and that they have met guidelines governing financial stability and commitment to quality."



TeleCheck, First Data's check and ACH acceptance business, is the first organization to become NACHA Certified. The business delivers industry-leading check acceptance and ACH payment solutions to financial institutions and businesses of all sizes, providing protection against fraudulent checks, verification and warranty services, streamlined processing, features to simplify back-office operations and convenient payment options for consumers.

"We are pleased to be the first company to be NACHA Certified. We have a track record of innovation in the industry including delivering the first point-of-sale check conversion at scale and being the first to accept checks from a camera on a point-of-sale device with Clover Check Acceptance," said Barry McCarthy, Executive Vice President, Head of Network and Security Solutions at First Data. "NACHA Certified recognizes our steadfast commitment and leadership in processing and securing ACH transactions."

For more information about NACHA Certified, visit www.NACHAcertified.org and for more information about Third-Party Senders, visit www.nacha.org/thirdpartysenders.

FRAUD continued from page 1

email account of a business executive through social media or other means, or creates an email account that is slightly different from the real one. The fraudster then sends an email requesting a wire transfer—possibly even emulating the business executive's writing style—to an employee with payables responsibility. The email usually conveys a sense of urgency.

The employee, thinking the online wire transfer request is legitimate, initiates the wire transfer with the company's financial institution. Because the request comes from an authorized account signer, the financial institution usually processes the transfer, and the business suffers a loss.

Though these wire transfer fraud incidents are easy to miss and on the rise, there are things you can do to protect your business.

- **Educate Your Employees.** Ensure all employees tasked with handling wire transfers are aware of these scams, and train them to scrutinize all transfer authorization emails. Make sure these employees inspect not only the sender's full email address, but also the body of the email. Red flag an email if it includes spelling errors, unfamiliar account information or addresses or if it deviates from the sender's usual style.
- **Confirm with a Call.** Ideally, even if a wire transfer request appears legitimate, your employees should confirm all email requests with the requestor in person or over the phone. This simple second step immediately identifies an imposter.
- **Release Regular Reminders.** Keep employees and co-workers aware of the ongoing risk for wire transfer fraud through company emails, newsletters and at business meetings. Properly train all new employees, and those who may serve as proxies when employees are on vacation, in the review process.
- **Set up a Second Security Level.** Talk to your financial institution about confirming wire transfer requests that exceed a pre-set dollar amount. Designate an executive or other employee the financial institution should call to confirm all requests of this size.

If you believe your business has been the target of wire transfer fraud, contact your financial institution, local law enforcement and the FBI's Internet Crime Complaint Center.

Source: Sun National Bank

Understanding OFAC Compliance: Why Your Business Needs to Be In the Know

With every passing year, the U.S. Treasury Department casts a wider net of Office of Foreign Assets Control (OFAC) violations, ensnaring everyone from unwitting small businesses to sophisticated corporations. The continual expansion of a global economy that trades increasingly online, across international borders and through digital currency is driving the Treasury's dedicated efforts to ensure all U.S. businesses comply with OFAC regulations that aim to thwart illicit activity and terrorism.

Increased Office of Foreign Asset Control (OFAC) Scrutiny Means:

- A single OFAC fine now commonly equals, or even dwarves, the total amount of fines OFAC once levied in a full year.
- Other business types are just as likely as traditional financial institutions to incur large citations, including seven- and eight-digit fines.
- The smallest fines imposed today are significantly higher than those of just five years ago.

Technology solutions provider Computer Solutions Inc (CSI) authored a white paper ***Understanding OFAC: A Best Practices Compliance Guide for All Businesses***. The white paper examines OFAC compliance, identifying best practices to help all business and industry types better understand and meet their OFAC compliance obligations, thereby avoiding costly penalties, damaged reputations and even potential criminal charges.

Comparing the Percentage of Fines Between Traditional Banks & All Other Business

Year	% of Fines Against Traditional Banks	% of Fines Against All Other Businesses
2016	11%	89%
2015	33%	67%
2014	26%	74%
2013	26%	74%
2012	31%	69%
2011	14%	86%
2010	22%	78%
2009	11%	89%

From 2006 to 2016, OFAC imposed $4.2 million in civil money penalties (CMPs). While financial institutions still typically incur the highest dollar fines, CMPs against other businesses, including non-traditional financial institutions, make up the majority of the total number of fines every year. In each of the last eight years, other businesses represented at least two-thirds of the total number of all OFAC fines imposed.

OFAC violations are costing U.S. businesses real money; while the largest concentration of fines fell in the $100,000 to $499,999 category (27%), in 2016 fines over $1,000,000 tied for the top spot. For any business, these fine amounts can cause considerable damage; and for a smaller business, they could spell catastrophe. Depending upon which program a business is determined to have violated, the consequence can be as high as $20 million in criminal penalties and 30 years in prison for willful violation.

A thorough review of recent years' OFAC enforcement actions uncovered 3 trends:

1. OFAC is going after small business with as much gusto as larger, more sophisticated firms. This was particularly true in 2014 and 2015, when OFAC specifically identified the fined entity as a "small business" in 21% of its enforcement actions.
2. An alarming number of enforcement actions noted that no OFAC compliance program was in place at the time of the violation.
3. Beyond the industries that have earned a "financial institution" designation

see OFAC on page 5

OFAC continued from page 4

under the USA PATRIOT Act, there are several other industries that are quickly and increasingly becoming the target of OFAC investigations and fines, including:

- Data Processing Services
- Energy and Fossil Fuel-Related Firms
- Electronic Payments and Trading Entities
- Retailers, Distributors, Suppliers and Manufacturers
- Transportation and Logistics Providers

Do you know what your business' regulatory obligations are in regard to OFAC? Simply stated, every U.S. citizen, permanent resident alien and company is prohibited from doing business with entities targeted on OFAC's Specially Designated National (SDN) list, which includes terrorists, narcotics traffickers and those controlled by or acting on behalf of sanctioned countries.

Any business transaction could potentially violate OFAC, and there is no minimum dollar amount. However, certain transactions pose a higher risk, including, but not limited to, those that are:

- Initiated from foreign countries
- Cash only, especially for large or luxury items that are easily liquidated
- International wire transfers involving international parties
- Real estate deals, especially where the borrower or seller isn't personally known
- Loan transactions, especially if the proceeds go to a third party
- With entities known to conduct business in sanctioned countries

To develop your own OFAC compliance program, which should be commensurate with your organization's risk profile, you first need to understand the basics about OFAC's sanctions programs and your responsibility to them.

The most important aspect of an OFAC compliance program is its denied party screening process. The Specially Designated Nationals (SDN) list is updated every time OFAC identifies a new individual or entity to be added or removed, which can be daily. Your risk profile will determine how often you need to cross-check that list; with every transaction, with every new customer, or your entire customer database at periodic intervals, for instance.

The white paper identifies five critical best practices:

- Use Outsourced List Updates
- Automate the Screening Process
- Support Multiple Integrations Methods
- Leverage Advanced Word-Matching Technologies
- Use an On-Demand Solution

Reading this informational white paper can be a first step to developing a viable and actionable compliance program that fits your organization. If you need further assistance, talk to your financial institution today.

Source: CSI

The U.S. Path to Faster Payments

The United States stands on the verge of a transformation in how businesses and consumers make payments. Rapid technological innovation; demand for faster, smarter payments; and the impressive will of the industry have collided to create an unprecedented opportunity. The Federal Reserve Banks' Faster Payments Task Force is calling on all payment stakeholders to take action and be part of this historic effort.

The vision for creating a faster payments system in the U.S. was unveiled with the release of ***The U.S. Path to Faster Payments, Final Report Part Two: A Call to Action***. In support of this release, a live online broadcast featured industry leaders from the Faster Payments Task Force discussing the task force's final report and its 10 recommendations for developing and implementing a faster payments system in the United States.

Building a fast, safe and ubiquitous payments network in the U.S. has and will continue to take unprecedented collaboration from every sector of the payments industry. Let's keep this impressive momentum going—be a part of this historic effort and show your interest and support.

Review the report for a wealth of information on what lies ahead as the payments industry works to create a secure, ubiquitous, faster payments system by 2020. **The Faster Payments Task Force website** shares even more resources for those looking to learn more.

Source: FasterPaymentsTaskForce.org

"THEY'RE HERE!"

Same Day ACH Debits Have Arrived

ACH debits became eligible for same-day settlement with the implementation of Same Day ACH Phase 2 on September 15, 2017. A NACHA ACH Operations Bulletin released in April provided information to Originating and Receiving Depository Financial Institutions, Originators, Third-Party Senders and software and processing vendors on important aspects of ACH debit processing in a same-day environment. Even those not planning to use same-day processing for ACH debits should take reasonable care to prevent unintentional same-day ACH debits.

Action Items

- All Originators should "check and correct" the Effective Entry Dates in ACH transactions they originate, even those that do not intend to make use of same-day debits.
- All Originators that intend to make use of same-day ACH debits should review their authorization language to ensure that the terms are clear and readily understandable regarding the timing of such debits.
- All Third-Party Senders, ACH software vendors, and ACH payment processors should assess their own role(s) in ensuring accurate ACH processing, including the accurate dating of ACH transactions.

Use Cases and Benefits of Same Day ACH Debits

There are a number of use cases for Same Day ACH debits that can provide substantial benefits for ACH participants, including consumers:

- Billing companies can offer same-day bill payment via their web sites and call centers, allowing consumers to have their bill payments made and completed on a single business day. This can include bill payments made on due dates; that are late; or are for the start, end, or restoration of service.
- Billers and merchants can accept and convert checks that settle on a single business day.

In these and other use cases for Same Day ACH debits, consumers may have access to more up-to-date information about transactions to their accounts, and therefore better information about their actual available balances. As the Consumer Financial Protection Bureau (CFPB) commented, "same day ACH may help alleviate some of the challenges consumers face today in trying to forecast when various types of credit and debit payments will post to their accounts and the complications - such as overdrawn balances, non-sufficient balances for subsequent payments, and fees - that can arise from such uncertainty."

As distinct from the use cases described above, the existing next-day ACH capability is likely to continue to effectively serve other use cases for ACH debit payments that are scheduled in advance. For example, pre-authorized recurring debits for insurance, utility or mortgage payments generally have an established payment schedule or monthly due date that is known to both parties in advance. Regardless of whether the biller in such cases uses next-day or same-day ACH debits, ultimately it is the biller's (Originator's) responsibility that the ACH debit settles no earlier than the scheduled settlement date.

Fully understanding the processing of Same Day ACH debits (intentional or unintentional) benefits the businesses using the service as well as the consumers on the receiving end. If you need further clarification on Same Day ACH, contact your financial institution.

Source: NACHA

Accepting Check Payments at Your Small Business

Small business owners can offer several payment options to their customers. One way to receive money is by accepting check payments. To broaden payment options for any company, they need to know how to accept personal checks.

How to Accept Check Payments

If a business decides to accept checks, they need to keep some key points in mind. Follow a few simple steps to collect valid checks and correctly deposit them.

- When receiving a check, verify that it was written for the right amount. The numerical amount and the written amount should be the same. Do not accept checks for more than the total amount due.
- The check must include personal and banking information. The following details should be correctly written or printed on the check:
  - Complete name of the payer
  - Current date
  - Financial institution ID numbers including account and routing/ABA numbers
  - Payee name (the business)
  - Dollar amount
  - Signature

Once the information is verified, deposit the check as quickly as possible. Obviously, the faster a check is deposited, the faster the business receives payment. Delaying a deposit might cause problems because some financial institutions won't allow checks to be deposited after a certain number of months (usually 6). Be timely with check deposits to maintain a healthy cash flow, and be minimize the possibility of not being able to collect on the check.

Check Acceptance Policy

Create a check policy if your business plans on accepting checks for payment. The check acceptance policy will help identify and avoid non-sufficient funds (NSF) checks at your business and should outline how staff handles check acceptance and deposits.

Train employees on the check acceptance procedures and how to handle checks. Be sure that everyone knows how to spot a bad check.

Accepting Checks Online

An online check, or e-check, is a type of electronic funds transfer processed through an ACH (automated clearing house) system. The payment is made through the internet or another data network.

Online check processing turns a paper check into an electronic transfer. The check is deposited into the business account automatically, resulting in instant payment.

E-checks are processed like credit cards but have lower fees. The consumer writes a paper check at the point of sale, and it is then scanned by a machine. The reader captures the information on the check (additional information can be entered to complete a one-time payment from the consumer's account.)

Accepting checks online can also be done through a business' website. A consumer enters the routing and financial institution account numbers, along with other relevant information. The check is processed online, and the business receives payment immediately. This makes it easy and convenient to accept electronic check payments from consumers.

Online check processing usually offers several security features for your business, including authentication, digital signatures, and encryption. Depending on the payment

see CHECKS on page 9

Understanding EMV Transactions Can Help Businesses Manage Liability

As more POS terminals are being upgraded to EMV chip-ready, and more financial institutions are getting chip cards in the hands of the consumer, questions regarding fallback transactions are being generated.

What is a Fallback Transaction?

Simply stated, a fallback transaction occurs when a chip card is presented to a chip enabled terminal ("chip-on-chip"), but the transaction is conducted as a swipe, usually due to the terminal unable to read the chip on the card. This could be due to a defective or scratched chip, a terminal or network incorrectly configured or with a chip reader that is defective (all legitimate reasons for fallback), or a chip intentionally damaged so it cannot be read, on a counterfeit card encoded with magnetic data stolen from a chip card.

When a terminal is properly configured, the process flow would be:

- The cardholder inserts the card (either because they initially knew to do so, or were directed by the terminal) but
- In this case, the terminal is not able to communicate with the chip on the card.
- After the terminal retries to read the chip (a pre-configured number of retries), the terminal will display a CHIP ERROR; USE MAG STRIPE message to the cardholder (sometimes reworded for cardholder display).
- The cardholder swipes the card, and the transaction is sent to the issuer for authorization.

Why it's Important to Understand Fallback Transactions.

Fraud liability is the main reason to fully understand fallback transactions. If there is counterfeit fraud involving a chip-issued card at a non chip-enabled terminal, then the merchant who did not upgrade the terminal is responsible for any fraud, meaning the issuer can chargeback the fraud to the merchant. However, if the terminal is enabled to read chip cards, but the transaction is conducted using magnetic swipe, then the issuer is responsible for the liability for fraudulent transactions, if the issuer authorizes the fallback transaction.

Is it Possible to Counterfeit an EMV Card?

For now, it will be extremely difficult to counterfeit or modify the chip. But if the fraudsters can get a hold of payment credentials (from a breach) then they can create a counterfeit card that looks like a real chip card, with the stolen credentials on the mag stripe. However, if the mag stripe data is counterfeit, more than likely the chip on that same card is altered, fake, or is from a stolen chip card and made to be unreadable. When the counterfeit card is inserted into the chip-enabled terminal, the terminal will not be able to proceed using EMV, and will most likely (depending on settings at the terminal) display instructions to swipe the card. If the issuer then authorizes the fallback transaction (it is coded as a

see EMV on page 9

Are You a Third-Party Sender?

If so, don't forget to conduct your **ACH Rules Compliance Audit** by **December 31**! EPCOR's *Third-Party Sender ACH Audit Workbook* will walk you step-by-step through the process and formulate a final report for you.

Or, if you would like an outside set of eyes, contact LarryM@epcor.org to schedule a professional audit with EPCOR.

EMV continued from page 8

fallback) and it is fraudulent, the issuer is liable for the fraud.

So Should Businesses Decline Fallback Transactions?

It is strongly recommended that businesses do not decline fallback transactions, not for the first one or two years. At least initially, there will be many legitimate reasons for fallback: valid but defective or otherwise unreadable chips, merchant terminals not configured properly, technical interoperability, etc. Based on observations from the EMV roll-out in Canada, legitimate fallbacks will significantly decline by the end of the second year, and issuers can begin to decline fallback.

How Can a Business Identify a Fallback Transaction?

If the terminal is configured correctly, the authorization request from the processor should be encoded with:

- Terminal Entry Capability 5 (chip device)
- Track 2 Equivalent Data Service Code (Digit 1) is 2 or 6 (chip card), and
- POS Entry Mode 02 or 90 (magnetic-stripe read)

It is these three items, when viewed together, which defines that a chip card, at a chip terminal, used mag stripe entry.

What Proactive Steps Can Businesses Take?

Monitor reports from your processor for fallback transactions. Several fallback transactions on a single cardholder may indicate a defective card, or the need for member education, or it may indicate a counterfeit card in use. Several fallback transactions from a single merchant may mean a terminal or a processor or a PIN debit network not properly configured.

Source: thepaymentsreview.com

CHECKS continued from page 7

processor, the check is verified at the point of sale. That way, you know if the check is good before the customer leaves your premises.

Pros and Cons of Accepting Check Payments

Accepting checks can be beneficial for many small business owners, but they can also carry some challenges. Take a look at the pros and cons of accepting check payments.

Pros of Accepting Checks

Lower Processing Fees

Personal checks usually cost a business less than credit and debit cards. To accept credit and debit card payments, you must use a card processor. Card merchants charge a percentage of each sale made on a credit or debit card.

Usually, paper checks do not have fees associated with depositing money. And, online check processing fees are lower than credit and debit cards.

Broaden Your Customer Reach

Checks could open your business up to a new customer market. Accepting checks at your business gives customers another payment option. Some people prefer to pay with checks. By accepting checks, customers don't need to carry a lot of cash or charge the amount to a credit card.

Increase Your B2B Sales

Certain kinds of customers tend to pay with checks more often than others. For example, many businesses prefer to pay their suppliers with checks. If you make mostly business-to-business sales, you might benefit from accepting check payments.

Cons of Accepting Checks

It takes longer to get cash

When a consumer pays with a paper check, you don't instantly have money in your hand or your account. There are extra steps to take to deposit the check. Accepting checks adds more to your to-do list and can take time away from other business tasks.

Checks can be inconvenient

Some consumers don't like check payments, carry a checkbook, or want to fill out checks to make purchases. If you limit options to accepting cash and check payments, you could end up turning away customers who want to use credit cards.

Not all checks are good

Sometimes, checks bounce because the account is closed or has insufficient funds. The business has to track down the consumer and collect payment from them. The collection process can be a hassle, and the business miight not ever be able to collect money for the bad check. This means the business doesn't get paid for the good or service you provided and may have to write off the amount as a loss.

Source: patriotsoftware.com

40% of Small Businesses Never Recover from a Disaster

One of the hard lessons many small businesses are learning after the devastating impacts of Hurricanes Harvey and Irma is that a disaster plan is essential — even if you think you'll never need to use it.

According to the Federal Emergency Management Agency (FEMA), almost 40% of small businesses never reopen their doors after a disaster. Recent data from a CNBC/SurveyMonkey Small Business Survey also shows that most small business owners don't spend too much time thinking about the environment as a critical factor.

Only 8% of business owners in the second quarter survey said the environment is the factor that most matters to them. The percentage goes down for business owners in the South Atlantic (5%) and West South Central (6%). Jobs and the economy, health care, terrorism, immigration and "other" ranked higher.

Meanwhile, business owners in the South Atlantic (64%) and West South Central (62%) said they expected revenue to increase in the next year, the highest level of sales confidence among owners in all U.S. regions.

Having a disaster plan in place might not prevent the worst-case scenario, but it could increase a company's odds of survival.

A little bit of work now can pay off down the road. Here are five things a small business may want to focus on.

Keep Your Company Records in the Cloud

Some disasters, like a hurricane, give you time to collect important items before you flee. Others, like a fire, offer no warning whatsoever. Things like invoices, contracts, tax returns, budgets and insurance policies are essential to businesses. And some will be critically important when you're dealing with an insurance company or applying for relief funds.

"A lot of small businesses don't have a process to protect themselves," said Mike Crincoli, president of The Neat Company, a document scanning/cloud storage company that caters to small businesses.

"Things like expenses and contacts and client data are very important, so it's essential they have a system to protect their records," he said. "It's very important to stay ahead of it."

Establish Policies for Employees, Vendors and Customers

The ripple effect of a disaster on a business can be easily overlooked, as owners focus entirely on rebuilding or reopening. Insurance might cover your immediate financial losses, but you'll also need to have a plan in place to hang onto customers and other business relationships during that rebuilding phase.

And you don't want to lose your best employees either, even if you're unable to pay them during the closure.

"News travels fast and perceptions often differ from reality," noted the Department of Homeland Security's Ready.gov website. "Businesses need to reach out to customers and other stakeholders quickly. Customers expect delivery of products or services on time. If there is a significant delay, customers may go to a competitor."

The American Red Cross suggests three separate plans for employees, suppliers and clients. For customers, be sure to have contact numbers for everyone and set up a communications infrastructure. Also, have a clear plan that's communicated to your workers on how their payroll and leave would be affected by a disaster.

For vendors, again, make sure you have all necessary contact information, and develop backup plans in case vendors are unable to get necessary products to you. (A disaster in their

see HURRICANE on page 11

HURRICANE continued from page 10

area that's nowhere in the area can still have significant impacts.)

When it comes to customers, keep the contact information of your most critical ones, so you can stay in touch with them during any period you're shut down. And try to have a plan in place to keep them supplied until you're back up and running.

Update all contact lists regularly and make sure they're accessible from any location. The important thing to keep in mind is it's critical to respond promptly, accurately and confidently to all of these groups. That can be tricky when you're dealing with the stress of an emergency, so Homeland Security noted it's best to have pre-scripted messages for each group—meaning you'll have to consider a number of different disaster scenarios and have the right messaging for each one.

Develop a Continuity Plan

The heart of a disaster plan is a continuity plan, since it helps businesses continue operating even after an emergency. First, identify which operations are essential (or time-critical), and designate which employees will carry those out. This may require some cross-training of employees in advance (which can also come in handy if an essential staffer leaves for another job).

The government suggests continuity plans be built using four steps:

- Conduct a business impact analysis to determine the most critical business functions.
- Develop recovery strategies to fill potential gaps brought on by an emergency.
- Work with a team, if possible, to develop the formal plan, as employees might think of weak spots the owner might miss.
- Finally, educate your entire staff about the plan and train them on their responsibilities.

Do a Threat Analysis

Business owners will want to factor in all potential hazards when creating their emergency plan. Some disasters, like fire and tornadoes, can happen anywhere. But it's wise to conduct a risk assessment of your businesses location to see what else could happen.

Is your geographical region prone to tornadoes? Are you within striking range of a major hurricane? Has there been any historic flooding? If you're in any sort of metropolitan area, have you considered terrorism? And don't forget cyber attacks. Too many small business owners actually downplay that threat: only 2% of the small-business owners surveyed in the CNBC/SurveyMonkey Small Business Survey said they view the threat of a cyberattack as the most critical issue they face.

Run Drills

A good plan is useless if no one knows how to execute it when disaster hits. Work with employees regularly to ensure things will run smooth in the case of an emergency, and have a loyal customer and vendor you can use as test subjects during those drills.

It may seem a waste of time, but if the unthinkable happens, it could mean the difference between a company's survival and an out-of-business sign.

Source: CNBC.com

epcor®

Electronic Payments Core of Knowledge

EPCOR is your electronic payments core of knowledge and influence. We are a member-focused association devoted to providing personalized support and services.

The mission of EPCOR is to provide our members with the knowledge, support and industry representation necessary to succeed in the ever-evolving electronic payments business.

NACHA DIRECT MEMBER
Regional Payments Association®

Through our direct membership in NACHA, EPCOR is a specially recognized and licensed provider of ACH education, publications and support.

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