What Small Businesses Should Know About EMV or Chip Cards

The U.S. is one of the last developed countries to migrate from magnetic-stripe ("mag-stripe") cards to EMV[8] or chip cards. The four major card brands (American Express, Discover, MasterCard and Visa) are leading the effort to move the U.S. to a chip-based card payments infrastructure. Affected are credit, debit and prepaid cards issued by U.S. financial institutions. This article addresses these commonly-asked questions about chip cards:

- What are the benefits of chip cards, and how will the migration to chip card technology affect payments fraud in the U.S.?
- How did the October 2015 fraud liability shift impact merchants?
- What is the status of the U.S. migration from mag-stripe to chip cards in terms of card issuance and merchant acceptance?
- What changes need to be made to POS terminals in order to accept chip cards?
- What factors should small businesses consider when deciding whether to accept chip cards?
- How can small businesses learn more about chip cards?

Benefits of Chip Cards and Impact on Card Fraud

The biggest benefit of chip card technology is the potential reduction in card fraud due to counterfeit and lost and stolen cards for card-present transactions (card-present transactions refers to sales in which the card is physically present at the POS and the merchant has the opportunity to inspect the card.) Chip card transactions offer enhanced functionality in cardholder verification and transaction authorization, thus potentially providing better security than mag-stripe cards.

A chip card has an embedded microprocessor chip (it looks like a small, metallic square on the front of the card) that stores information securely and performs cryptographic processing during the payment transaction.

When a chip card is manufactured, the chip is encoded with security credentials that are extremely difficult to counterfeit. Notably, the chip creates dynamic data that are unique for each transaction and these data cannot be used again, thus diminishing the value of stolen card data. Because of these security features, countries that have implemented chip cards have seen a reduction in card-present fraud rates.

Traditional mag-stripe cards, in comparison, carry static data that does not change from one transaction to the next. Criminals steal the data from the mag-stripe and use it to create fraudulent transactions. For example, criminals may install devices to skim card data at automated fuel pumps or Automated Teller Machines (ATMs) and then use that card data to make fraudulent purchases.

In card-not-present (CNP) transactions (such as telephone, mail orders and internet sales), the merchant doesn't see the actual card. EMV technology does nothing to protect against fraud in CNP transactions. Countries that have migrated to chip cards have seen CNP fraud rates increase. Criminals who are thwarted by the more secure card-present transaction environment that comes with chip cards may turn their attention to the CNP environment where the pickings are easier. Similarly, cross-border counterfeit fraud (particularly ATM fraud) rates have grown in countries that have moved to chip cards. Card issuers, merchants, card brands, cardholders and others should consider implementing a variety of potential solutions[9] to help mitigate or prevent CNP fraud.

Fraud Liability Shift

A major incentive for merchants to prepare for chip card acceptance is the shift in liability that took effect in October 2015. Previously, under the card brands' operating rules, the card issuer was liable for financial losses due to counterfeit card fraud. With the liability shift, a merchant will bear the loss if the issuer has issued chip cards to its cardholders and if that merchant has not been certified through its acquirer as being EMV-compliant (by having implemented payment terminals that can read chip cards and taking other compliance steps).[10]

[8] EMV, which stands for Europay, MasterCard and Visa, is a global standard for integrated circuit or chip cards. The EMV specifications define a set of requirements to ensure interoperability between chip-based cards and terminals throughout the world.

[9] EMV Migration Forum, "Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud," April 2015, available at www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/. This white paper is an educational resource on best practices for authentication methods and fraud tools to secure the CNP channel as the U.S. migrates to chip technology.

[10] The principle is that the party (issuer or merchant) that is the cause of a contact chip transaction not occurring (and thus falling back to a magnetic stripe transaction) will be financially liable for any resulting card-present counterfeit card losses.

Also in October 2015, MasterCard, Discover and American Express shifted the liability for a lost or stolen card to the party with the highest risk environment. Within that hierarchy, chip and PIN verification is considered more secure than chip and signature. If neither or both parties are EMV compliant, the fraud liability remains the same as it is today.

Migration Status

Forecasts vary, but it is estimated that about half of the 1.2 billion U.S. payment cards included EMV chips at the end of 2015, and most of these were credit cards.[11] Several payment industry commentators have predicted that by 2020 more than 90 percent of U.S. cardholders will have an EMV card. Debit card issuance has increased significantly since the beginning of 2015, now that debit routing challenges have been resolved. According to the 2015 Pulse Debit Study, 90 percent of surveyed financial institutions said that they plan to start issuing EMV debit cards by fourth quarter 2015 and will complete their transition by the end of 2017.[12]

As for merchant readiness, industry experts estimated that about 30 percent of POS terminals were capable of accepting chip card transactions at the end of 2015. To date, it is primarily the largest retailers who have installed chip-enabled terminals. While a large retailer may be able to make a sound business case for investing in chip card technology at the POS, a smaller retailer may not be able to do so as readily. Smaller merchants with relatively low card transaction volumes may find that the expenses associated with chip card upgrades are greater than simply accepting liability for the low levels of fraud they might experience from fraudulent mag-stripe transactions. One survey found that smaller retailers are slower to equip for EMV acceptance, with merchant respondents indicating that they felt upgrading terminals was not necessary, too expensive and/or that they were not concerned about the fraud liability shift.[13]

Accepting Chip Cards at the POS

Many POS terminals purchased in recent years are already EMV-capable, but that functionality is not turned on; it is necessary for merchants to get the necessary software installed, tested and certified before they can process chip card transactions. Depending on the market, there may be a long wait for installation, testing and certification services.

As a small business, is it advisable for you to invest in POS terminals or upgrades so your business can accept chip cards? Investment in chip-card acceptance equipment may be worthwhile if:

- You accept card payments today in "card-present" situations, or you plan to do so in the near future
- A significant portion of your sales is to strangers (versus people you know and trust), making your business more vulnerable to counterfeit and lost/stolen card fraud attacks
- Card payments are a significant percentage of your total sales
    - However, if most of your card transactions tend to be telephone orders or internet purchases (CNP transactions), it may not be cost-effective for you to invest in chip card terminals

Another consideration is the time and resources needed to train your staff and educate customers on the use of chip cards. In addition, some consumers may perceive that chip cards offer better security. Merchants that don't accept chip cards could be at a disadvantage if they are viewed as a less secure option for that consumer, potentially eroding customer confidence and reducing loyalty.

It is important to realize that nearly all chip cards (whether issued in the U.S. or elsewhere) will continue to carry mag-stripes for the foreseeable future, and the U.S. payments infrastructure will continue to support mag-stripe technology for many years to come. Thus, merchants will still be able to accept card payments (and process them with mag-stripe technology) even if their POS terminals are not equipped to accept chip card transactions.

To Learn More about Chip Cards

Small businesses can prepare for the move to chip cards by learning more about issues, costs and arming themselves with facts to support informed business decisions. The cross-industry EMV Migration Forum's website, www.emv-connection.com, has an excellent, informative Knowledge Center, and www.gochipcard.com is another website that provides useful information. Seek out information from card brand representatives and card brand websites, and confer with bankers, merchant acquirers and card processing service providers to inform your decision on whether and when to accept chip cards. See the Resources section of the Small Business Payments Toolkit on page 36 for additional links to information about chip cards.

[11] http://newsroom.mastercard.com/press-releases/more-than-575-million-u-s-payment-cards-to-feature-chip-security-in-2015/

[12] PULSE 2015 Debit Issuer Study Executive Summary.

[13] Wells Fargo/Gallup Small Business Index, July 2015.

Small businesses can think of "alternative payments" as payment methods that exist outside of mainstream legacy payment channels such as checks, ACH transactions and payment cards.

This article will focus on examples of alternative payments that utilize online and mobile delivery channels; a high-level description of virtual currency is also included. The introduction provides an overview of issues that small businesses should consider when contemplating moving to an online or mobile environment for their payments and banking needs. Then, more detailed examples of alternative payment solutions are provided, including: remote deposit capture; PayPal; Level Up; Square; and, in the virtual currency section, Bitcoin.

Introduction

The payments system is constantly changing, enabling businesses to utilize new ways to make and receive payments. Some businesses have moved beyond paper payments, such as checks and cash, and rely on credit and debit cards or the ACH system to make and receive payments. However, technology is improving access to payment services for consumers and businesses alike. Web-based and mobile options are expanding the payment services that businesses can access and expanding the ways businesses can initiate a payment. Most online and mobile innovations focus on consumers, but business services are gaining traction. Small businesses are already active users of banking and financial services via online and mobile channels—e.g., lending, account balances, statements, invoices, payments, etc. Online and mobile "payments" are mainly new ways to access existing payment infrastructure, including card networks, the ACH system, wires and even checks. In this article, we begin by providing a checklist of what small businesses should consider if they are thinking of moving to an online or mobile environment for payments.

Checklist before Moving to an Online or Mobile Environment

- Do your research: What payment needs do you have; what pain points do you want to reduce; and what benefits do you hope to gain for customers, for suppliers and for your business?
- Cost-benefit analysis
- Make the case to leadership
- Assess and organize IT resources needed (internal or vendor)
- Leverage current IT systems, relevant banking and vendor services, and online and mobile systems
- Actively promote new payment method to customers, suppliers and trading partners (offer incentives and rewards)
- Plan and implement change, understanding that this may take time

Things to Look for from an Online or Mobile Solution Provider

- Small business-focused online and mobile banking services
- Integration services—i.e., linking your payments with accounts payable (A/P) and accounts receivable (A/R) systems and other financial systems
- Remote deposit capture
- Fraud monitoring and prevention tools, including alerts
- Clearly explained fee structure (per transaction, monthly costs, chargebacks)
- Interest in understanding/meeting your needs rather than selling their solutions

Talk to Your Banker

- Be proactive in contacting your bank about payment needs; don't expect bank to contact you
- Seek out a small business and/or payments expert for help (this will likely be someone other than your loan officer)
- Bring specific information about payments needs or problems you're trying to solve—e.g., emerging products you have investigated; current systems you use; pain points
- Conduct due diligence on data security and compliance requirements for mobile/online products
- Ask about risk mitigation services offered by the bank; implement those that make sense for you, for example, fraud/risk education, fraud and risk alerts and so on (many of which are free)

Getting Started in an Online Environment

Before migrating to online payments, many businesses explore online financial services offered by their bank via online banking products. For example, businesses might take advantage of online bill pay products. If a small business chooses to be paid via online bill pay, it must work with its bank to be added to the relevant biller directory, along with pertinent payment instructions. As a payer, a business can control when the payment is withdrawn from the account. Online bill pay is usually free to use.

There are obvious benefits to being able to access services such as online bill payment and transaction history. However, there are some potential concerns. For example, when using online bill pay, businesses should keep in mind that they are not protected by Regulation E (Reg E)[14] in the same way as consumers. If an online business account is hacked and a fraudulent payment is issued, the business may be liable for the loss. Dual controls[15] are not usually offered, so online bill pay might be vulnerable to employee fraud. In general, when considering online payments, businesses should be aware of some of the many different schemes that are used in cyber-attacks against business information and accounts. Accounts payable, payroll and cash management are targets. Examples of fraud schemes include: phishing; use of company information and personally identifiable information (PII) obtained from websites and social networking sites; and data breaches that are orchestrated to obtain information about a company, its vendors, and customers. For more on payments fraud, refer to pages 20 to 25 of this Toolkit. These are all things for small businesses to keep in mind as they consider approaching their banker about the use of online services.

As noted above, many small businesses begin to access online solutions through services such as online banking and bill pay. There are other newer innovations in online payments that businesses may access as well. While many online payment solutions have focused on the consumer space, progress continues to be made in the business-to-business market. Today, there are a variety of options for small businesses to consider when moving to an online payment environment. For example, Amazon Payments® integrates into a business' existing website; customers can pay using information stored in their Amazon.com accounts. Another option is authorize.net, which is a payment gateway service provider that works with a business' existing merchant account to accept credit cards and electronic checks through its website. Many small businesses are familiar with Intuit's Billing Solution for QuickBooks. This service integrates directly with QuickBooks and allows a business to get paid online via credit card from any invoice generated.

Detailed Example: PayPal®

In 2015, there were 173 million active PayPal accounts.[16] PayPal allows small businesses to accept online payments without having a traditional merchant account; customers don't need a PayPal account to pay. PayPal charges its business and premier account holders a per-transaction fee, plus a percentage of the transaction. Through PayPal business services, businesses can accept credit cards online or by phone; they can also create and track invoices through a PayPal account. The system has recurring payment capabilities.

PayPal features include:

- Ease of setup and use
- Customer familiarity
- No merchant account needed
- Customers don't need a PayPal account to make a payment
- Businesses can create and send invoices through PayPal account
- Capability of setting up recurring payments
- Can be integrated with other shopping card systems

Concerns include:

- PayPal's Seller Protection policies do not cover digital goods[17]
- Cost of chargebacks
- Time for funds to clear
- Limits of terms of use policy
- PayPal is not regulated in the same way that banks are regulated; protections differ
- Fees for currency exchange

PayPal also has a mobile/cloud tokenization[18] solution: the consumer opens a mobile app, authenticates with the payments services provider (PSP), and requests an offline payment token.

[14] Regulation E or Reg E provides a basic framework that establishes the rights, liabilities and responsibilities of participants in electronic fund transfer systems such as automated teller machine transfers, telephone bill-payment services, POS terminal transfers in stores and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments). The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer or magnetic tape that instructs a financial institution either to credit or to debit a consumer's asset account. Source: www.federalreserve.gov/bankinforeg/regecg.htm

[15] Dual controls means requiring more than one person to act to make payments on behalf of a business.

[16] Source: www.statista.com/statistics/218493/paypals-total-active-registered-accounts-from-2010/

[17] Digital goods are intangible goods that exist in digital form, such as e-books or webinars.

[18] Tokenization is the process of substituting sensitive data with unique identification symbols (a "token") that retain all the essential information without compromising security. The token has no extrinsic or exploitable meaning or value.

Mobile Banking and Payments for Small Businesses

In addition to payment and banking products offered online, there are a variety of services that small businesses can access using mobile devices such as smart phones and tablets. These include access to account information, alerts, collection of card payments via attachable appliance or app, the ability to make payments and remote deposit capture of checks. It is difficult for many small businesses to accept credit card payments. Some companies face challenges related to obtaining the infrastructure necessary for credit card processing. For this reason, some small businesses have hesitated to utilize card payments. However, software app and card-swiping devices provided by payment vendors (e.g., Square, Intuit) have increased access to card payments for small businesses. These alternatives are marketed to small merchants as ways to accept low-value credit/debit card payments at fixed rates.

Many of the same considerations that were outlined above regarding online payments also apply to mobile payments. The convenience and increased access brought about by mobile payment options goes hand in hand with considerations for how to ensure that payments are secure. In addition to the issues discussed in this toolkit regarding payment fraud on pages 20-25, small businesses should take into consideration what types of authentication and encryption tools are included in the mobile payment solutions they are implementing. When developing a mobile payment platform, it is especially important to consider access controls in order to limit the entities that see and store data transferred via a mobile transaction.

A few examples of mobile payment solutions are provided.

Detailed Example: Remote Deposit Capture (RDC)

RDC lets small business deposit checks for collection with their bank electronically. Benefits include:

- Fast and easy, saves time and cost of trips to the bank
- Later cut-off time to get checks deposited
- Quicker access to funds

If check volume is small (less than five checks per day), businesses would most likely deposit one at a time. The business would photograph the check with a smart phone camera and use its bank's mobile app to deposit the check "image" electronically, usually for immediate availability. If the business receives more than five checks per day, the business would deposit batches of checks together. To do this, the business must first acquire a scanner from its bank (these can be rented or purchased for about $200 and up) and scan in checks. Then, the business would need to create a batch file and transmit the batch electronically to its bank to deposit checks remotely. Both versions require pre-enrollment and sometimes a credit check must be performed.

Detailed Example: Square

Square uses mobile apps through phones for Android™ and/or Apple® to allow buyers to pay via card (Square accepts Visa, MasterCard, American Express and Discover) at places like farmers markets, restaurants, festivals and other venues with small merchants. Square utilizes equipment (the "dongle") and apps that are fairly easy for small businesses to "plug in" and use; examples of how Square works are included below. Moreover, Square does not require a merchant account, unlike most credit card companies. Square accounts are linked to merchants' bank accounts, and deposits into those accounts are usually available in one or two business days. Square charges businesses a flat rate per swipe plus a percentage of each transaction; rates are higher for manually-keyed transactions.

Square offers merchants a variety of ways to access card payments:

- Square Reader: This is a small "dongle" that attaches to an iPhone® or smartphone for Android's headset jack; the Square app is used to access payment capabilities. Customers can swipe the card and enter their PIN or provide a signature right on the phone screen. A Square Reader can be obtained for free.
- Square NFC/EMV Reader: Square has partnered with Apple to allow merchants to accept Apple Pay® (and other contactless mobile payments) and EMV chip payments. It can be used in place of or with the Square Reader and uses the same app to process payments.
- Square Register: The Square Register app allows merchants to use the Square Reader on an iPad® or tablet for Android to move beyond processing card payments. Square Register allows a variety of services such as: accepting cash payments; sending digital receipts and invoices; and processing transactions offline, among other services.
- Square Stand: This alternative allows a merchant to turn an iPad into a stationary POS system at the checkout. The Square Stand has a built-in reader that can be turned to face the merchant or the customer.

Detailed Example: LevelUp

The free LevelUp mobile application for iPhone and Android, developed in 2011, relies on the ability of mobile device cameras to "read" QR (quick response or bar) codes. This innovation is not dependent on mobile device hardware that includes near field communication (NFC), so LevelUp can be used with a variety of devices. LevelUp allows registered users to securely link their debit or credit card to a unique QR code displayed within the app. To pay with LevelUp, users scan the QR code on their phone at LevelUp terminals located at local businesses that accept LevelUp as a form of payment. LevelUp uses BrainTree® and Bank of America® for payment processing and charges a flat fee for that processing.

LevelUp provides a variety of services, including full-scale POS solutions with varying hardware costs. Every merchant that accepts LevelUp as a form of payment also offers monetary savings to users. Users are given "First-Time Visit Specials" the first time they make a transaction at the merchant's location. Users can also unlock "credit" to a merchant's store after spending a certain amount at the merchant's location. There are currently more than 1.5 million users of LevelUp, with 14,000 businesses enrolled.

Even Currency is Going Digital! Understanding Virtual Currencies

Virtual currency (also referred to as digital currency) can be defined as a type of stored-value product or digital money that is issued and usually controlled by its developers, and is used and accepted among the members of a virtual community. Virtual currencies are not issued by a federal government ("fiat currency") or backed by a central bank. Consequently, virtual currency is generally unregulated. There are currently more than two hundred virtual currencies in use, of which Bitcoin is the largest and most well-known. Small businesses that are thinking about moving to electronic payments should consider whether or not accepting virtual currencies as a form of payment makes sense for them.

Virtual currencies, which are non-fiat digital moneys normally controlled by their developers, fall into three categories: closed schemes, unidirectional and bidirectional:

- Closed currencies are not exchangeable with traditional currencies (an example is World of Warcraft® gold).
- Unidirectional currencies are bought with traditional money or can be earned by participating in activities (Amazon Coins are an example) but cannot be converted back to fiat currency.
- Bidirectional currencies are purchased with traditional money and can be converted back to traditional money; they can be used to buy virtual and non-virtual goods. Bitcoin is an example of bidirectional virtual currency. This is the only type of virtual currency that might have the potential to compete with traditional currency. Bitcoins act as currency in that they can be used as a means of payment, a method of exchange, a store of value and a unit of account.

Virtual Currency Example: Bitcoin

Bitcoin, a virtual currency system with no central authority at its core, was launched in 2009. It permits the transfer of currency online, directly, anonymously and outside government control. Bitcoin has attracted much attention from computer developers, venture capitalists and merchants who see it as an alternative to traditional payments. Transactions take place using complex mathematical algorithms and elliptic-curve cryptography, including digital signatures, open source computing methods and peer to peer networks. Transactions are recorded in the "blockchain," a public ledger and proof of every Bitcoin transaction that has ever occurred. New Bitcoins are created through "mining," as a reward for applying computing power to verify new transactions. The average person can't really be a Bitcoin miner, because of the computing power now required. Instead, people buy and sell Bitcoin on a number of exchanges, privately through peer-to-peer contact. Some people who are interested in Bitcoin don't exchange it for currency at all, but offer goods and services for Bitcoin.

Bitcoin can be divided to eight decimal places (to a "satoshi" currently worth less than 1/1,000 of a cent) so that it can accommodate so-called microtransactions for low-value transfers. Today, about 15.3 million Bitcoins are in existence. A finite supply of 21 million Bitcoins will be created through mining, at which point the total amount of Bitcoin in circulation will no longer increase; it will likely decrease slightly as some people will inevitably lose their private keys, essentially destroying the Bitcoin they owned by locking it away forever. Because of this feature, some people call Bitcoin "deflationary by design," meaning that it is intended to appreciate in value over time, assuming increased adoption makes it relatively more scarce. When miners are no longer rewarded for operating the network by newly created coins, they will rely entirely on transaction fees (which are a relatively small portion of revenue today, and just a fraction of the cost of traditional payment networks).

Some merchants accept Bitcoin as payment today. Examples include:

- Overstock.com -- since Bitcoin payments save the retailer credit-card fees, Overstock™ offered an incentive to customers paying with Bitcoin; 1% back on purchases (in-store credit)
- Microsoft® accepts Bitcoin payments for a variety of digital content
- Dell® allows customers to buy computers and hardware with Bitcoin
- DISH Network® has announced it will allow customers to pay for their television programming packages with Bitcoin
- Expedia® accepts Bitcoin for hotel bookings (but not for flights, yet)
- Square's online marketplace, Square Market
- Many others accept Bitcoin payment directly; other retailers offer their dollar-denominated gift cards through online sellers (like Gyft) who accept Bitcoin.

A key barrier to the acceptance of any virtual currency is the desirability of actually holding revenue denominated in that currency. Most merchants contract with an exchange (e.g., Coinbase®), that converts consumers' Bitcoins into dollars and transfers dollars to the merchant. Bitcoin does not allow chargebacks and Bitcoin transaction costs are generally cheaper than those with credit/debit cards: the fee for a service like Coinbase is around 1%. However, the transaction fee to Square Market merchants for payments with Bitcoin remains the same as the fee charged for all other Square Market transactions.

Bitcoin is more than a currency: it also acts as a payment system. Transactions are tracked and audited for legitimacy through open-source code; they are final and irrevocable. There are also escrow services to mediate transaction disputes between buyers and sellers. Because it is decentralized, some tout its advantage in cross-border transfers, which are processed as easily as domestic payments. One can envision Bitcoin as an extension of other innovations that have changed the payment system, such as Amazon, PayPal and Square.

Issues to Consider

Some observers have identified potential benefits and risks associated with virtual currencies such as Bitcoin.

Potential Benefits of Virtual Currencies

- May reduce risk of identity theft
- Has immunity to conventional inflationary pressures and sovereign risk
- Gives potential access to financial instruments for those who are unbanked
- Might have lower transaction costs for merchants
- Settles almost immediately
- Provides irrevocability and finality
- Is accessible to anyone with access to a computer or smart phone
- Contains security features that are created through digital signatures and cryptography
- Useful in countries where social or political climate may lead to distrust of local currencies or there is a high degree of connectivity to the internet
- Opportunities in areas like notary services and tracking asset ownership

Potential Risks of Virtual Currencies

- May allow for a level of anonymity that can lead to criminal activity
- Can require a lot of computing power and electrical energy to complete a transaction because the calculations that assure trust between unfamiliar parties are rigorous
- Has no central authority providing a natural bridge to the currency and no guarantee of value
- Many provides no recourse for owners who lose money through fraud, exchange collapse, or simple transaction errors and lost "passwords"
- Is treated differently than other currency by regulatory bodies. For example, in the U.S., the Internal Revenue Service (IRS) has said that Bitcoin and other virtual currencies will be taxed like property, not currency.
- Faces an uncertain legal status. Regulations are still forming and inconsistent and some nations are attempting to outright ban the use of virtual currency.
- Is not ubiquitous

Despite issues and challenges, virtual currencies aren't going anywhere. Virtual currencies are difficult to repress due to their decentralized structure. Some observers think virtual currencies could ultimately change not only the traditional financial system, but also the way we transfer and record financial assets like stocks, contracts, property titles, patents and marriage licenses. The same design features that allow virtual currencies to exchange value without relying on a central record-keeper make it possible for virtual currencies to be used for anything for which we have traditionally used a trusted "middleman" for verification. For example, in 2015, at a hotel at Walt Disney World®, a couple used a Bitcoin ATM to record their written marriage vows on the blockchain. Major stock exchanges and even government property records offices are already experimenting with these networks for recording and transferring ownership of stock certificates and property titles. Others are finding ways to use the networks to create "smart contracts" that can function as automated escrow services and more. Increasingly, industry experts believe that decentralized currencies might not become major factors themselves, but that the technology underlying their creation will transform traditional money and financial services and find application across a range of industries that manage identity, ownership, privacy and contracts.

Business Continuity Planning for Small Businesses

Business Continuity Planning

On May 22, 2011, one of the top 10 deadliest tornadoes in the U.S. to date tore through Joplin, Missouri. This was the third tornado to strike Joplin since 1971 and the event included multiple vortexes and 200 MPH winds. Over 17,000 insurance claims were filed with over $2.2 billion paid. Would your business survive such an event? How would you and your employees work around the loss of major city infrastructure, power, phone, water outages, and internet? How would you react to hazardous conditions including natural gas leaks and harmful spills?

"Locating the business was a challenge: no landmarks, street signs, or visual reminders remained. There were no phones and no internet. Cell service was spotty; at least texting was often successful. It was difficult to find our office when there were no street signs."

– From October 2012 EPCOR presentation "Business Continuity Planning: Lessons from the Joplin Tornado" by representatives of Commerce and Arvest Banks.

According to the Institute for Business and Home Safety, an estimated **25 percent** of businesses do not reopen following a major disaster. You can protect your business by identifying the risks associated with natural and man-made disasters, and by creating a plan for action should a disaster strike. By keeping those plans updated, you can help ensure the survival of your business.

Business continuity is your plan to keep working despite almost any disruption or disaster. It involves the ability to keep or get your processes and information back up and running as soon as possible. This can be accomplished by something as simple as restoring a backup to a new computer (so your whole system is back the way it was), all the way up to using a virtual service with your backup in the cloud. Business continuity is a must for companies of all sizes. The ability to quickly get your system working on current or new devices can ensure your business will survive not only the event, but the potential long-term effects.

Disaster recovery is the ability to get back to normal operations in the event of a disaster. A disaster can be anything from a storm or flood that destroys your office to a breach of your sensitive networks or a compromise at your point-of-sale. Disaster recovery is really just a plan to put the information critical to your business onto new computers and/or servers.

Backing up your data must be a priority for your disaster recovery planning; your backups are what you're going to use to recover after the disaster occurs. Backups can include a variety of methods: files, directories, image backup, cloud storage, etc. It is common to experience a hardware or software failure causing you to lose your data. Backing up information from your PC regularly is recommended so you do not lose important information. This practice can also protect you from fraud issues such as malware used to hold your data hostage for a ransom. This may also include backing up the data on your mobile devices, such as photos and contacts.

"Locating the business was a challenge: no landmarks, street signs, or visual reminders remained. There were no phones and no internet. Cell service was spotty; at least texting was often successful. It was difficult to find our office when there were no street signs."

Remember: What you backed up determines what you can recover.

Planning ahead for a business-threatening event should include an "all hazards" approach. There are many different threats or hazards. The probability that a specific hazard will impact your business is hard to determine. That's why it's important to consider many different threats and hazards and the likelihood each will occur. Strategies for prevention/ deterrence and risk mitigation should be developed as part of this planning process. Threats or hazards that are classified as "probable" and those hazards that could cause injury, property damage, business disruption, or environmental impact should be addressed.

Write out our plan and testing strategies. Once you've identified the key factors in your recovery and continuity planning, it's time to start setting up your plan. Begin by establishing requirements and objectives for your disaster recovery plan and capturing them in a written policy document. A preparedness policy that is consistent with the mission and vision of the business should be written and disseminated by management. The policy should define the goals and objectives of the program, and roles and responsibilities. The policy should authorize selected employees to develop the program and keep it current. Each of your major stakeholders needs to review the document and edit it as needed. You'll also want to establish testing processes and periodically review your strategy. In general, it's a good idea to test your backup strategy once a quarter just to make sure that everything is running smoothly and to verify that no significant changes are needed. Persons with a defined role in the preparedness program should be trained to do their assigned tasks and all employees should be cross-trained so they can take appropriate protective actions during an emergency.

What should a business continuity plan outline?

- Who is responsible for testing?
- What will be restored in a test?
- When tests will take place?
- How backup will be restored?

Before disaster strikes, have conversations with your banker, accountant, and other financial services providers to find out what their disaster recovery plans are. Online banking services such as bill pay, remote deposit services, or even credit card access can help your business function from any internet or mobile connection. Determine how they will support your ability to recover from disasters in order to assure the continuity of your small business.

Disaster Recovery is a lot like insurance – you hope you never need it but you want to make sure you have it if you do. While natural disasters, such as hurricanes and floods, tend to grab more attention, most forms of data loss and downtime have nothing to do with weather. Don't overlook threats such as fraud, water damage or fire.

Learn more about preparing a disaster recovery plan for your small business by exploring the business continuity resources listed on page 37.

Resources

Glossaries of Payment Terms

First Data Payments Industry Glossary: www.firstdata.com/downloads/thought-leadership/Payments-Glossary.pdf

TR-43-2014 Remittance Glossary:
A Publication of the Remittance Coalition
www.x9.org/wp-content/uploads/2014/02/TR-43-2014-Remittance-Glossary.pdf
Vocabulary and terminology reference guide that defines 169 terms related to payables and receivables processing, business to business payments and remittance handling.

Cardinal Commerce Payments Glossary: http://info.cardinalcommerce.com/payments_a_to_z

Accounting payment terms: www.accountingtools.com/accounting-payment-terms

Credit and Debit Card Resources

PCI stands for Payment Cards Industry.

PCI compliance information for merchants: www.pcisecuritystandards.org/pci_security/why_security_matters

PCI DSS Quick Reference Guide:
Understanding the Payment Card Industry
www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

PCI Information Supplement:
Best Practices for Implementing a Security Awareness Program
www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Purchasing card basics: www.napcp.org/?page=PCardIntro

Recommended Communications Best Practices is a step-by-step resource for issuers and merchants to develop effective messaging and education approaches during the U.S. migration to chip technology.
Available on the EMV Connection website at www.emv-connection.com/recommended-communications-best-practices/

Advice on best practices for card acceptance:
www.squareup.com/help/us/en/article/5079-best-practices-for-accepting-payment-cards
www.transfirst.com/resources/whitepapers/tips-for-preventing-fraud-and-avoiding-chargebacks

EMV Cards or Chip Cards Resources

General information about chip cards:
www.gochipcard.com
www.emv-connection.com

Technical specifications for EMV: www.emvco.com

Information for merchants about chip card acceptance from the major card brands:

American Express: www209.americanexpress.com/merchant/services/en_US/payment-EMV

Discover: www.discovernetwork.com/chip-card/merchants/index.html

MasterCard: www.mastercard.us/en-us/merchants/safety-security/emv-chip.html

Visa: https://usa.visa.com/dam/VCOM/download/merchants/Visa-Merchant_EMV_Chip_Acceptance-2014-07-17.pdf

Examples of Information for small merchants from payments processors:
www.chasepaymentech.com/faq_emv_chip_card_technology.html
www.heartlandpaymentsystems.com/wp-content/uploads/2015/08/EMV-and-Small-Merchants-White-Paper.pdf
http://info.vantiv.com/rs/vantiv/images/emv_what_smbs_should_know_about_emv_whitepaper.pdf

Resources

ACH Resources

National Automated Clearing House Association website (NACHA): www.nacha.org/

Direct payment via ACH: www.electronicpayments.org/small-business/direct-payment/learn/how-it-works

How to accept ACH payments: www.wikihow.com/Accept-ACH-Payments

Same Day ACH:

Learn more about Same Day ACH: www.frbservices.org/resourcecenter/sameday_ach/index.html
www.resourcecenter.nacha.org/

Watch the video "Same Day ACH: How Will You Benefit?": www.youtube.com/watch?v=K_XsiQ_54B0

Companies that Provide Payroll Services:
To find and compare payroll service providers, conduct an internet search using terms such as: payroll vendor comparison, payroll vendors reviews, payroll company comparisons, payroll service cost comparison, online payroll services reviews, outsource payroll service providers, compare payroll service companies, list of payroll providers, best online payroll service for small business, etc.

ACH Checklists and Forms

Direct Deposit of Payroll via ACH

"Get Started Toolkit" is a checklist explaining the steps to implement direct deposit of payroll via ACH:
www.electronicpayments.org/sites/electronicpayments.org/files/downloads/Direct_Deposit_ImplementationChecklist.pdf

Sample form for employees to sign to start having pay checks directly deposited into checking and/or savings accounts:
www.electronicpayments.org/sites/electronicpayments.org/files/private/Sample-DD-and-Split-Deposit-Form-OnePageFINAL2013.pdf

Direct payment via ACH

"Get Started Toolkit" is a checklist of steps to follow to get paid and make payments electronically via ACH:
www.electronicpayments.org/sites/electronicpayments.org/files/downloads/Direct_Payment_ImplementationChecklist.pdf

Sample direct payment authorization form:
www.electronicpayments.org/sites/electronicpayments.org/files/downloads/Sample_Direct_Payment_Authorization.pdf

General Small Business Resources

America's Small Business Development Center: http://asbdconline.globalclassroomportal.com/

America's Small Business Development Centers' website features an e-learning center with over 1,400 online business courses and video tutorials. A free membership offer is available.

Small Business Administration: www.sba.gov/
Follow this path to useful resources about payments: www.sba.gov/ » Starting & Managing » Managing a Business » Running a Business » Managing Business Finances & Accounting.

Business Continuity Planning:

www.sba.gov/managing-business/running-business/emergency-preparedness/emergency-preparedness

www.preparemybusiness.org/

www.ready.gov/business/implementation/IT

Fraud and Data Security Resources

Dun and Bradstreet "How to Help Prevent Payroll Fraud":
www.nfib.com/article/7-steps-to-preventing-payroll-fraud-57312/

Federal Communications Commission's Ten Cybersecurity Tips for Small Business:
https://apps.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf

Visit www.fcc.gov/cyberplanner to create a free customized Cyber Security Planning guide for your small business and visit www.dhs.gov/stopthinkconnect to download resources on cybersecurity awareness for your business.

Chamber of Commerce's Internet Security Essentials for Businesses:
www.uschamber.com/sites/default/files/legacy/issues/defense/files/020956_PDF_web.pdf

Council of Better Business Bureaus' Data Security Made Simpler:
www.bbb.org/data-security/

Business Know-How's "Are Employees Stealing from You? Tips to Prevent Employee Theft":
www.businessknowhow.com/manage/employee-theft.htm

Association of Certified Fraud Examiners "Small Business Fraud Prevention Manual" ($59.00):
www.acfe.com/products.aspx?id=2155&terms=(small+business+fraud+prevention)+
This is a book providing information on the most common internal and external fraud schemes committed by customers, employees and vendors against small businesses, as well as tips on how to prevent these schemes from happening to you. Highlights include: cash receipts and disbursements fraud; inventory and merchandise thefts; employee fraud prevention techniques; check and credit card fraud; vendor fraud; and fraud perpetrator prosecution. Explains what to do if your small business becomes a victim to fraud, including avoiding liability when conducting investigations and taking civil actions against perpetrators.

"Payments Fraud Liability Matrix" and "2014 Payments Fraud Survey Summary of Consolidated Results" are available at:
www.minneapolisfed.org/about/what-we-do/payments-information

The Association of Certified Fraud Examiners (ACFE) offer free fraud resources: www.acfe.com/free-resources.aspx

ACFE "Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study":
www.acfe.com/rttn-occupational.aspx
It includes a section on methods used to detect fraud in small businesses, as well as summarizing the frequency of fraud schemes by industry.

The International Association of Financial Crimes Investigators (IAFCI) offers general education in "Fraud Smarts: A Practical Guide for Online Safety":
www.iafci.org/Public/Public_Awareness/Community_Cautions.aspx In addition, select the small business icon on the left of this page to see fraud prevention tips for small businesses, including how to create a cyber security plan.

Common Fraud Schemes
The Federal Bureau of Investigation (FBI) lists the most common scams that the FBI investigates and offers tips to help prevent being victimized by fraud at the following link. It covers common fraud schemes, investment-related scams, internet scams and fraud targeted to senior citizens. You can sign up for email updates from the FBI on breaking news and other topics.
www.fbi.gov/scams-safety/fraud/fraud

Bank Holidays

Standard Federal Reserve Bank Holidays

Holiday*	2016	2017	2018
New Years' Day	Jan 1	Jan 2	Jan1
Martin Luther King, Jr. Day	Jan 18	Jan 16	Jan 15
President's Day	Feb 15	Feb 20	Feb 19
Memorial Day	May 30	May 29	May 28
Independence Day	Jul 4	Jul 4	Jul 4
Labor Day	Sep 5	Sep 4	Sep 3
Columbus Day	Oct 10	Oct 9	Oct 8
Veteran's Day	Nov 11	Nov 11*	Nov 12
Thanksgiving Day	Nov 24	Nov 23	Nov 22
Christmas Day	Dec 26	Dec 25	Dec 25

* For holidays falling on Saturday, Federal Reserve Banks and Branches will be open the preceding Friday. For holidays falling on Sunday, all Federal Reserve Banks and Branches will be closed the following Monday. Source: www.frbservices.org/holidayschedules/

Bank Holidays
Federal Reserve Bank holidays: www.frbservices.org/holidayschedules/
International bank holidays: www.bank-holidays.com

Regional Payments Associations

Regional Payment Associations (RPAs) serve member banks, credit unions, thrifts, municipalities, payment technology providers and businesses. Their services vary, but for the most part they all provide information, education, publications, operational support, advocacy and resources on Automated Clearing House payments as well as on other payment systems such as check and image; credit, debit and prepaid cards; wires; and payments-related risk and fraud.

Regional Payments Association	Website	General Territory Served
EastPay	www.eastpay.org	Florida, North Carolina, Virginia and West Virginia
EPCOR – Electronic Payments Core of Knowledge	www.epcor.org	Arkansas, Indiana, Kansas, Kentucky, Missouri, Nebraska, Oklahoma, Ohio, Illinois, Iowa, Pennsylvania and West Virginia
MACHA – the Mid-Atlantic Payments Association	www.macha.org	Maryland, the District of Columbia, Delaware, Northern Virginia, Northeast West Virginia and Southern Pennsylvania
NEACH – New England Automated Clearing House	www.neach.org	New England
PaymentsFirst	www.paymentsfirst.org	Alabama, Georgia, South Carolina and Tennessee
SHAZAM, Inc.	www.shazam.net	
Southern Financial Exchange	www.sfe.org	Alabama, Arkansas, Louisiana, Mississippi, and Tennessee
SWACHA – The Electronic Payments Resource	www.swacha.org	Texas, Louisiana and New Mexico
The Clearing House Payments Authority	www.thepaymentsauthority.org	
Upper Midwest ACH Association	www.umacha.org	Upper Midwest
WACHA – The Premier Payments Resource, Wisconsin Automated Clearing House Association	www.wacha.org	Wisconsin
WesPay – Western Payments Alliance	www.wespay.org	Western states

Resources

Health Care

ACH Primer for Healthcare

NACHA – The Electronic Payments Association published an "ACH Primer for Healthcare: A Guide to Understanding EFT Payment Processing" that introduces the healthcare industry to the Automated Clearing House (ACH) Network, explains ACH transaction flow and applications and includes two "next steps checklists," one each for origination and receipt.

https://healthcare.nacha.org/ACHprimer

Healthcare Electronic Funds Transfer (EFT) Standard

This fact sheet, published by the NACHA – The Electronic Payments Association, explains that the Patient Protection and Affordable Care Act (ACA) mandated the identification of a healthcare EFT standard, which was ultimately identified in 45 CFR 162.1602 as NACHA's ACH CCD+ Addenda. Providers can request delivery of claims payments via the healthcare EFT standard and health plans must comply. This fact sheet outlines the benefits of using the healthcare EFT Standard, explains how to enroll to receive the Healthcare EFT Standard, explains what is meant by EFT, and explains characteristics of EFT payment options for healthcare payments including ACH, virtual card and wire transfer.

https://healthcare.nacha.org/sites/healthcare.nacha.org/files/files/NACHA%20HC%20Fact%20Sheet%20-%20Revised.pdf

Webinars

View webinars on the Small Business Payments Toolkit on www.FedPaymentsImprovement.org and YouTube.

"How to Leverage the Small Business Payments Toolkit"
www.youtube.com/watch?v=rhYSXD3YJYA

"How Financial Institutions Can Leverage the Small Business Payments Toolkit"
www.youtube.com/watch?v=Qh7oGYS5E9c

"How Small Businesses Can Leverage the Small Business Payments Toolkit"
www.youtube.com/watch?v=cFQyIqdf8bY

"FedACH Services" is a registered service mark of the Federal Reserve Banks. A complete list of marks owned by the Federal Reserve Banks is available at www.FRBservices.org.

Other product names and company names referenced within this document may be either trademarks or service marks of their respective owners.

References to Third Parties and Third-Party Products or Services
The Federal Reserve Banks do not sponsor, endorse or recommend any third party or any third-party products or services referenced within this document.