By Linda Windler, Thoroughbred Systems, Inc.

Computer Corner

When Social Distancing Becomes Business Distancing – Today's Utility Payment Method Options

We hear a great deal these days about 'Social Distancing'. In fact that subject was mentioned in our last Computer Corner article:Like the Boy Scouts Have Always Said... "Be Prepared"! This article is about Tech Preparedness.

The "Computer Corner" article in the July 2020 issue of *The Kansas Lifeline Magazine* was intended to provide information and ideas a utility system could implement to help assure uninterrupted business, even during some sort of crisis. The article covered topics like RWD boards and city councils doing business through virtual meetings. The article also explained practices that would fall under the heading of "Working Remotely", i.e., working, say from home, rather than the office. This included advice like sharing of data over the Internet, using PDF printing (Portable Document Format), and saving stored computer documents, rather than physically printing reports. Also covered were methods to secure and protect those documents and data.

In that article, under the heading "Working Remotely", the last two items reviewed payment methods that do not require direct contact and are often well received by a public that is increasingly interested in automated or easy access ways of paying bills.

One of those bill payment methods is ACH (Automated Clearing House). We have just discovered a typo in the last article listing ACH as standing for American Clearing House. Perhaps it could be called that just as well because the U.S. government does have a long list of rules in place regarding this practice to make it a safe, secure way of transferring money. We do have to laugh sometimes, that even though there is supposed to be a hard and fast, a one way to do things set of rules, the interpretation of those rules has made for a number of slightly different methods. As programmers, we have to meet those demands while still making sure that the spirit of the rules is followed – the spirit being security.

The last item on that list was another remote payment method – Internet Pay. While both ACH and Internet pay were mentioned in the article, there is so much to know about each and so much to be considered that we promised readers that the next "Computer Corner" article, this article, to provide information concerning payment options.

Water System Payment Options:

"Ease of Payment" and "Customer Service" are top priorities. But there are many factors to consider including Quality Customer Service, Clerk Safety, Health Safety, Liability, Costs, and more.

Graphics by Linda Windler.

The Following is a list ranging from some timely considerations regarding traditional payment methods to newer high tech payment choices:

1. In Person: Cash, Check, or Debit/Credit Card Payments

Collecting large amounts of cash can make a clerk a target for crime. In 2020, direct clerk to customer contact must now include provisions to minimize disease transmission risk to both.

Protection of the office staff from both "Physical Harm" and "Health Risks" are responsibilities of the RWD Board and City Council. Steps should be taken to protect the office staff from physical attack or health risk and virus exposures during "in person" contacts. Over many years working with utility systems we could tell stories of clerks seriously threatened with physical harm, stalked and, yes, even attacked. And, these were not large metropolitan areas; these are small communities where people normally feel safe.

As a Board or Council member, do a web search of "bank safety", "security drive-up", "security cashier", or, "ticket windows and drawers". Surprisingly, it doesn't necessarily take a king's ransom to provide some extra security. New and used protection equipment is readily available from bank drawers ($100+ used) and Intercom systems ($50+ new). Even previously installed bulletproof glass in available inexpensively. New, top of the line bank quality systems cost from $1000 to $10000. If the situation requires the customer to enter the office to conduct business, is there a physical barrier, cashiers window, or some other form of separation and protection?

2. Deposit Box Cash or Check Payment Drop Box

There many relatively secure options readily available for $50+ including secure "through the wall" boxes for $200+. Discourage the deposit of cash, as it encourages break-ins. And, there's always a problem with someone claiming to have deposited cash that the clerk did not receive, or cash left without identification.

3. Mail-in Cash or Check

Cash payments are discouraged as the mail can be lost or stolen and the mail leaves no possibility of a proof of payment receipt.

4. Over The Telephone (OTP) – Debit/Credit Card Processing

"Over The Phone" (OTP) Card Payments is another service some utilities offer to their customers. The first step would be to contact the utility's local bank or credit card company about what Debit/Credit Card processing options they have available. There are thousands of options; as many businesses want to process those transactions and get "their cut" of the water system's money.

Common popular options include:

- Credit Card Company - Merchant Services Card Processing
- Local Bank - Card Processing Services
- Paypal - (Paypal.com)
- Square - (Squareup.com)
- Website Hosting Service Payment Gateways

All these, and similar options, allow for credit/debit card over the phone taking of payments to be entered directly into a desktop card terminal, computer or mobile phone device.

Be sure to ask about all Fees ...

- Are there Annual Fees such as: PCI (Payment Card Industry) compliance fee?
- Are there Monthly fees such as: equipment or software subscription?
- Is there a 'per transaction' fee?
- Does the fee vary dependent on the type of card or transaction?
- Is the Transaction Fee a Fixed rate, a percentage of the transaction or combined fee?
- Is a contract required?

Federal Law and Security Standards . . .

Federal law in the United States does not require compliance with the PCI Security Standard. However, Visa and MasterCard both require merchants and service providers to be validated according to the PCI Standard.

Information from the PCI Security Standards Council has a laundry list of recommendations:

- Only process credit cards using a PCI Compliant Service Provider.
- Never store the CID/CVV2 card security code in any format (three digit number on card back).
- Never store the magnetic track data from any card, in any format, in any way, ever.
- Encrypt ANY electronic storage of full credit and debit card numbers. (Better yet - just don't store.)
- Do not store cardholder data in computers or on paper.
- If you must store cardholder data, keep any paper documents containing a full credit card number in a secure location (locked file drawer/safe) when not in use.
- Allow only employees with a business need to have access to credit card numbers.
- Don't share user IDs and passwords.
- Immediately change passwords and disable access for all terminated employees.
- Use strong passwords. Be sure to change default passwords on hardware and software.
- Secure all business computers by installing and activating personal firewalls, virus and malware protection software, and disabling all generic or default user accounts and passwords.
- Make sure any wireless routers are password-protected and use encryption.
- Secure and regularly examine all POS swipe devices for signs of tampering.
- Create a security policy that addresses all aspects of the PCI standards.

If anyone has more than 20,000 online transactions per year, they fall into a category with even more stringent security requirements.

See PCI SS Council website for more information: https://www.pcisecuritystandards.org/

In today's world of online hackers and crime, Web security is a constantly moving target. A September 14, 2020 news clip in The Wall Street Journal gives evidence: "Regulators Prepare to Reprimand Citigroup for Failing to Improve Risk Systems. Federal regulators are preparing to reprimand Citigroup Inc. for failing to improve its risk-management systems – an expansive set of technology and procedures designed to detect problematic transactions, risky trades and anything else that could harm the bank."

Use Web Tools such as Glary Utilities and CCleaner to help clear out browser cache and cookies to reduce risk of accidental sensitive data exposure.

- ❖ Is there a Contract or Term Requirement, if so, is there a cancellation of contract fee?

5. Recurring (Monthly) Automatic Payment by ACH or Credit Card

The NACHA (National Automated Clearing House Association) system processes electronic funds-transfers "ACH" payments each night while America sleeps. Recent rule changes now allow most transactions made using ACH to clear on the same business day. ACH is usually the easiest and least expensive method to safely provide automatic recurring bill payment services to customers, as most banks provide ACH processing as a free service to their municipal and rural water system utility customers.

Most utility billing software companies offer options to efficiently generate a transmission ready file for authorized customer bills to be sent to the bank for automatic ACH payment processing from checking or savings accounts.

We have sometimes discovered folks have the misunderstanding that ACH can only apply to those customers that bank at the same bank as the utility system. Nothing could be farther from the truth. It is no different than taking paper checks in that regard, except, the bank does less work because they don't have to have a person key the information off of a paper check into a computer, it is already there.

NEVER accept the legal liability for these transactions by handling them on the utility system's website, which certainly could be hacked! Instead, sign up with a reputable payment processing service. Let these payment professionals handle the security, PCI compliance, and liability protection needed. Only place a "Pay My Bill Now" button on the utility system's website that links to the payment processing service.

NEVER put sign-up screens on the website for ACH Autopay or Credit/Debit Card payment. Instead, only place a printable PDF form on the website for customers to download or print and fill out in order to sign up for services. Warn customers to NOT send back such information over email, which is totally unsafe.

6. Some Common (to our region), Customer-Initiated Online ACH or Credit Card Payment Options include:

- Local Bank - Bill Payment Services
- KanPay - (https://kic.kansas.gov/)
- Paypal - (Paypal.com)
- PayStar - (https://home.paystar.co/)
- Payment Services Network - (paymentservicenetwork.com)
- Website Hosting Service Payment Gateways

Most website hosting services provide an option to process credit card payments as a feature of their web hosting plans. There are hundreds of Web Hosting Services. Some of the more popular ones are: Bluehost.com, ionos.com (1&1), InMotionHosting.com, and GoDaddy.com.

Get complete information before purchasing a plan from the hosting provider or gateway.

Find out the details concerning customer convenience, ease of use, fees, liability/responsibility, and security. Is an SSL (Secure Sockets Layer) Security Certificate included?

An SSL certificate is a MUST if the intent is to process secure online payments. If the website is hacked or compromised, where does the responsibility lie – with the utility system or the payment gateway service? Are the fees reasonable? These are all questions that need answers in arranging for the acceptance of payments.

If not using their own "personal bank" bill payment system, caution customers to MAKE SURE to ONLY pay bills on the utility system's legitimate website. Customers should be warned about locating the site through a 'Search'. They should make sure they are going to the one and only link that is actually the city or district's site.

The world of today gives people more options for methods of conducting business than ever before, but it pays to educate oneself in order to make good choices.

Water systems have been known to experience "Website Spoofing" in which unknown persons create a website intended to trick customers into paying their bill on the "spoof site'. These "fake/spoof" websites often appear legit with photos and logos copied from the real website and typically charge the customer unreasonably high fees for processing the payment. People end up on these sites when they let their browser do a "Search" based on whatever few words they type in to find the site, then they pick what they think looks like it rather than using a specific link to go straight to the site.

In many cases, details of credit card transactions are stored in the browser, although it isn't considered safe. Use Web Tools such as Glary Utilities and CCleaner to help clear out browser cache and cookies to reduce risk of accidental sensitive data exposure. A savvy web user will always look for the lock icon in a web browser that indicates a secure mode of encrypted communications is in use. This indicates a type of connection designed to prevent others from reading or modifying the data exchanged with the website.

The world of today gives people more options for methods of conducting business than ever before, but it pays to educate oneself in order to make good choices.

Merle Windler and his wife Linda are owners of Thoroughbred Systems, Topeka. The company specializes in software solutions for utilities and municipalities, computer networking and associated training. Contact: merlewindler@yahoo.com