Using Your Smart Phone as a Credit Card Substitute
by Ira Wilsker

Forget your wallet.

Use our app like a wallet to pay at the counter, from the table, or from around the corner, your order is in your hands. Or simply select PayPal at the register to log in and pay, just like online.

Get Our App

Find a store location near you

Chantal Guillon
444 University Ave, Palo Alto

Tell the cashier:

I'm paying with PayPal.

You're checked in securely.

1. Open our app, find your store and check-in.
2. Choose how to pay and order, even if you're not there yet.
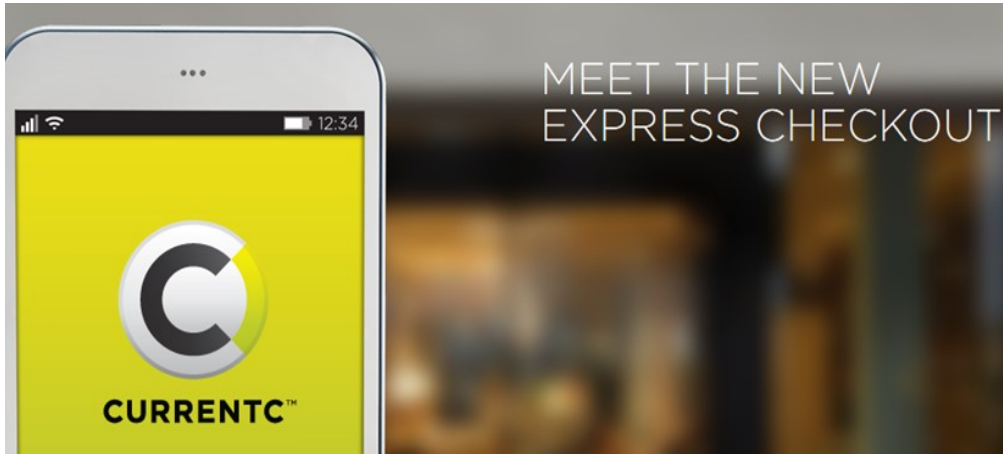3. Step up to get your order without getting out your wallet.

WEBSITES:

https://www.paypal.com/us/webapps/mpp/pay-in-stores
https://www.paypal.com/us/webapps/mpp/store-locator
http://www.pcworld.com/article/2846535/a-guide-to-the-top-mobile-payments-options.html
http://www.apple.com/apple-pay/
www.mercurynews.com/business/ci_26938386/mobile-payments-apple-pay-google-wallet-and-otherhttp://currentc.com
http://www.pcworld.com/article/2607312/how-

http://currentc.com
http://www.pcworld.com/article/2607312/how-apple-pay-could-make-the-target-and-home-depot-breaches-a-thing-of-the-past.html
https://www.gosoftcard.com
https://wallet.google.com
https://www.google.com/wallet/shop-in-stores/
http://www.mastercard.us/cardholder-services/paypass-locator.html

MEET THE NEW EXPRESS CHECKOUT

CURRENTC™

It should be news to no one that over the past year there have been massive data breaches at thousands of retail locations. In my case, over the past year, my bankcard issuers have initiated the replacement of four credit cards and a debit card (one major credit card was replaced twice). Since I carefully review my monthly credit card statements for questionable activity, I am fairly confident that although several of my accounts were compromised by the massive retail data breaches, there have been no illicit transactions posted to any of my accounts.

Following last year's massive Target data theft, the media played up the fact that most credit and debit cards in the United States are still using the obsolescent magnetic stripe technology in order to process "POS" (Point of Sale) transactions. It is the vulnerability of this magnetic stripe data, and the methods used to process the digital transactions, have made such transactions vulnerable to cyber attack. As the American credit and debit cards were purloined by the hundreds of millions,

the number of European credit and debit cards that were hijacked was much smaller. For the past several years, the majority of European (and many Asian) issued cards have had a more secure embedded microchip that contained the customer information, rather than the magnetic stripe widely used here. As overseas POS terminals (and many ATMs) were modified or replaced in order to take advantage of the more secure microchip technology, most domestic POS users have often been reluctant to implement the enhanced security technologies citing the massive capital investment in the current generation of magnetic stripe POS readers. Looking at my recently replaced credit cards, all have the embedded chip, as well as a magnetic stripe.

These data breaches and the related vulnerabilities have obviously caught the attention of our domestic technology industry, as in recent months there has been a flurry of technological advancements that may offer most of us the opportunity to mitigate the risks of a somewhat insecure plastic credit or debit card. While much of the media fanfare has gone to the introduction of Apple's Apple Pay electronic payments system (apple.com/apple-pay), others have been active in promoting their respective systems including eBay's PayPal,

SECURITY AT EVERY LEVEL

Passcode Protected
A personal 4-digit code ensures only you can access your account.

Paycode Protected
Every transaction is guarded by a secure Paycode that's unique to every purchase.
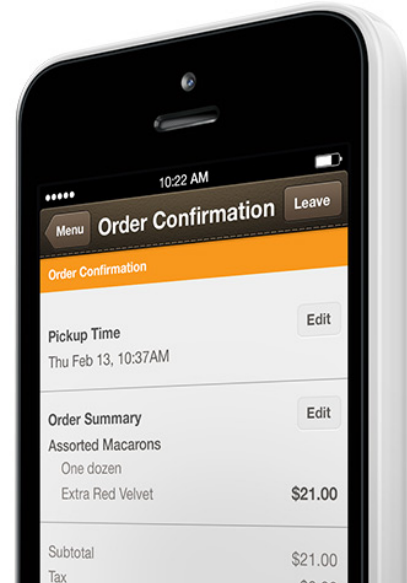
Cloud Protected
Your information lives on our highly encrypted cloud – so it's never shared or stored on your phone.

Order over chaos.

Order ahead so you can get your goodies and get on with your day. No signing, no lines. You can even use the app to order and pay at the table in some locations. Check please.

Google's Wallet, CurrentC (a joint effort of Sears, Target, and WalMart, CVS, and others), GoSoft-Card (joint effort of American Express, Chase, and Wells Fargo), and several others. While there are some variations in the technologies utilized by each, they are all designed to allow the use with a smart phone or related device to make secure retail transactions without the use of a traditional plastic credit or debit card.

      With its outstanding ability to promote itself, Apple has had much of the media spotlight with its recently announced Apple Pay system. According to Apple, "Paying in stores or within apps has never been easier. Gone are the days of searching for your wallet. The wasted moments finding the right card. Now payments happen with a single touch. Apple Pay will change how you pay with breakthrough contactless payment technology and unique security features built right into the devices you have with you every day. So you can use your iPhone, Apple Watch, or iPad to pay in a simple, secure, and private way." What garnered the most attention is a feature of the iPhone 6 devices (also present on many other recent smart phones) called "NFC" or "Near Field Communications". This is a very short range radio technology that allows digital devices to communicate with each other when held physically close to each other. Again, ac-

cording to Apple, "One touch to pay with Touch ID. Now paying in stores happens in one natural motion - there's no need to open an app or even wake your display thanks to the innovative Near Field Communication antenna in iPhone 6. To pay, just hold your iPhone near the contactless reader with your finger on Touch ID. You don't even have to look at the screen to know your payment information was successfully sent. A subtle vibration and beep let you know." Other Apple devices, without the NFC capability can use the Apple Pay app along with an integral finger print reader (part of the Apple Pay app) to complete a financial transaction without presenting a plastic credit card. Apple Pay requires that one or more established credit card accounts be linked to Apple Pay, with the user having the option to select which credit card will be used to process the Apple Pay transaction. By default, the credit card linked to the user's iTunes account is the primary credit source, but other cards can be securely added to the account. PayPal, one of the world's most widely used digital payment systems, recently introduced its own smart phone app that can be used for in-store POS transactions (paypal.com/us/webapps/mpp/pay-in-stores), without the use of a plastic credit card. According to PayPal, "Forget your wallet. Use our app like a wallet to pay at the counter, from the table, or from around the corner, your order is in your hands.

The way to pay with your phone

Pay for purchases by adding participating credit cards from **American Express, Chase®,** or **Wells Fargo®** to Softcard or setting up an **American Express Serve®** Account that you can add money to with your preferred debit card, credit card or U.S. bank account.[†]

American Express

American Express Serve

Chase

Wells Fargo   ⟩

Debit and Other Cards

Wells Fargo Cards

Add your Wells Fargo Credit Card to Softcard. Tap and pay anywhere Visa payWave contactless payments are
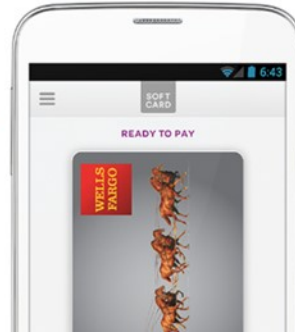
smart phones, as CurrentC does not incorporate NFC. Instead of using NFC, which is not available on most of the existing smart phones, CurrentC displays a unique bar code or QR type of image on the phone screen that is scanned by the cashier; every transaction will have a unique image displayed. CurrentC is designed to connect directly to the consumer's bank account, bypassing the credit card fees imposed by the bank cards on the retailers. Like many of the existing individual store cards and loyalty cards, CurrentC can take advantage of the personal information entered by the user when the account is created. Since CurrentC will have some personal information, incentives, rewards, coupons and other promotions may be offered the user. CurrentC will implement a "Save, Earn Pay" service where users will automatically receive offers, coupons, and other incentives from the participating retailers (Save); get instant points and rewards from participating loyalty programs (Earn); and combine and coordinate between checking accounts,

store gift cards, and selected credit and debit card (Pay).

I predict that as these new technologies become more widely implemented, we will see the number of mass data thefts decline, saving the financial institutions (and their millions of account holders) from substantial losses. We will also see these payment systems evolve and improve as they become more widely accepted, along with the inevitable failure of some. We may see consolidations (mergers) among some of these systems, and some may simply cease to exist as they find that they cannot successfully compete in the market place.

Whatever happens with these new payment systems, it appears likely that our traditional plastic credit cards may become as obsolescent as paper checks have become, and these new technologies will reign supreme ... until some newer technologies make these obsolete. In terms of POS payment technology, this will be an interesting couple of years.

Meet Tappy!

Softcard's new spokesperson.
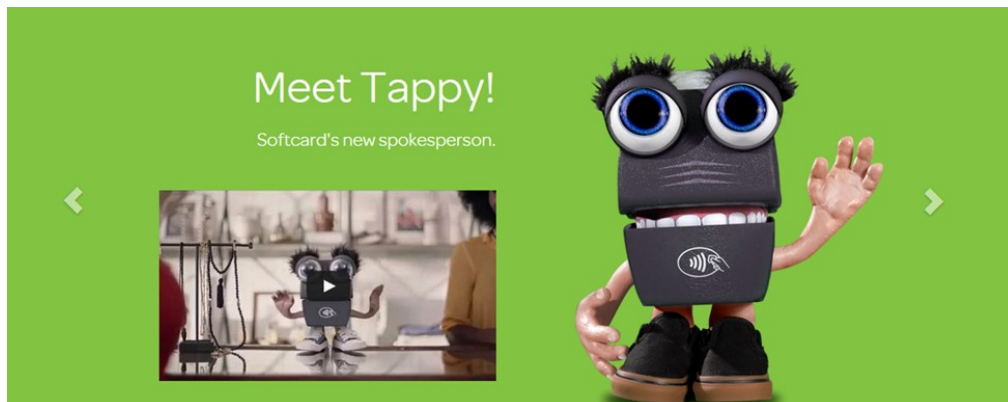
Or simply select PayPal at the register to log in and pay, just like online." Experimenting with the PayPal Store Locator (paypal.com/us/webapps/mpp/store-locator), using the Examiner's zip code (77701), there were about 75 nearby businesses that accept payments with the PayPal app including Home Depot, Dollar General, OfficeDepot, American Eagle, Aeropostale, ToysRUs, Academy Sports, and a variety of medical offices, florists, clothing stores and boutiques, restaurants, retailers and service businesses. Traditional PayPal transactions are connected to an existing bank account or credit card for ultimate payment.

A consortium of major banks, along with the major cell phone companies have created an app "SoftCard" which enables users to digitally enroll their existing credit cards issued by American Express, Chase, Wells Fargo, and many other institutions in to their SoftCard app. SoftCard, which is a free app for Android and Windows Phone, requires a compatible smart phone with NFC (Near Field Communications) in order to converse with the POS devices. Many smart phones will need an advanced SIM card, which is designed to securely store and protect sensitive payment information; generally, the participating cell phone carriers will replace an older SIM card with the newer advanced card at no charge. The user adds participating credit and debit card information to the device, which securely stores the information. Some prepaid cards can also be incorporated into the SoftCard app. Existing loyalty plans, membership and rewards benefits, and other features of existing credit cards are maintained when used with SoftCard. Special offers that may be available from participating merchants and credit card companies will be displayed on the phone when in proximity of the merchant. One example, listed as I type this, is

American Express offering a $1 cash back bonus, in addition to any other rewards, for each SoftCard transaction utilizing American Express.

Google wants very badly to compete in this lucrative field, and had developed an advanced digital "Wallet" (wallet.google.com) that can utilize a secure app that can be used for a variety of transactions. For users with NFC compatible phones, that feature can be used at many retail locations; for those without a compatible phone, Google Wallet offers a secure plastic Google Wallet Card which is accepted domestically wherever a Debitor credit card, using the same PIN number as card as the Wallet account. Google requires that an existing card be linked to the Wallet account. As with most of the competitors, any rewards or loyalty points affiliated with the linked card will continue to be earned. Google Wallet can be used almost anywhere that Master Card is accepted, meaning that there are millions of locations that already accept it. The NFC feature of Google Wallet can be used anywhere that MasterCard PayPass is used (mastercard.us/cardholder-services/paypass-locator.html).

Several of the largest retailers, including Target, WalMart, and Sears, CVS, and RiteAid have created a consortium under the moniker "CurrentC" (pronounced like the money "currency"). Several of these retailers have already announced that they will not be accepting Apple Pay, and possibly some of the other smart phone based payment systems. Projected to be widely available by early 2015 as these and other retailers implement the system, CurrentC works differently than the other smart phone payment systems, as the free app will work on almost all smart phones, as CurrentC does not incorporate

Fairfax October Meeting

October 18th was a beautiful Fall day, but we had a good turnout for the Fairfax meeting.

Nick Wenri presided over the PATACS Annual Meeting election of Officers that preceded the general meeting with OPCUG. Nick established a quorum, including e-mail Ballots. There were no nominees from floor. The membership elected the slate of candidates: James Rhodes, President; Ron Schmidt, 1st Vice President; Mel Mikosinski, 2nd Vice President; Paul Howard, Treasurer; Bill Walsh, Secretary.

Several topics came up during the General Meeting Question & Answer session.

There was discussion about the Raspberry Pi (http://www.raspberrypi.org/) and similar low-cost (under $100) microcomputers. If you or someone you know can give a presentation on this topic, please e-mail director2(at)patacs.org.

A member had questions about upgrading to a new Verizon FiOS router and updating his wireless network from Wired Equivalent Privacy (WEP) to WiFi Protected Access II (WPA2) encryption. WEP is not secure; WPA2 is the current recommended setting to prevent unauthorized eavesdropping and network access. See http://www.verizon.com/Support/Residential/Internet/fiosinternet/Networking/Setup/QuestionsOne/123890.htm.

Has anyone used Amazon's CreateSpace service (https://www.createspace.com/) to self-publish a book? This is another potential presentation topic if someone has experience with this service.

Recommendations on Password Management software? There was discussion about LastPass (https://lastpass.com/) and the pros/cons of cloud-based password management services. See October 2014 issue of PATACS Posts for an article about password managers, and the September issue article about Mitro password manager.

The George Mason OLLI ID("G number") is good for education discounts at the Apple Store.

Mel Mikosinski gave a slide-based Learn 30 presentation about Zoom Video Teleconferencing (http://zoom.us/) that PATACS and OPCUG uses for meetings (one member from Maryland was participating in this meeting using Zoom). Paul Howard gave the introduction, explaining how PATACS experimented with several cloud web conferencing services before selecting Zoom. Participants can both view and give presentations over Zoom. The meeting host can transfer screen sharing to other participants.

PATACS objective is to reach members unable to attend live meetings in person. The current PATACS limit is twenty-three end users (service cost to PATACS is $99 per year with no additional cost to members), but Zoom has service plans that allow up to one thousand users. Adding another one hundred participants would cost an additional $99 per year. There is no fee per meeting nor limit on number of meetings. 1-to-1 meetings (such as person to person) are free, and the software application (Microsoft Windows, Apple OS X and iOS, and Google Android supported) is free. PATACS added the Room Connector feature (http://zoom.us/roomconnector) for $499 per year to allow use of room teleconferencing systems like the one at OLLI's Tallwood campus.

Mel explained how to setup and connect to a Zoom meeting. Zoom requires that participants setup an account and activate it by clicking a link delivered via e-mail. Each Zoom meeting has a unique nine digit number. The same sign up and password on one device will work on all devices. However, you cannot sign in on more than one device simultaneously; log out from one device before logging into another device.

Zoom offers dial-in (audio only) phone numbers for 1-to-1 (not group meeting) calls, but these incur additional charges.

Some tips for end users using Zoom for PATACS meetings:

PATACS provides Zoom meeting number and the Zoom meeting link in the e-mail

Install Zoom software updates before joining the meeting.

Turn off sending video to improve network performance.

Join the Zoom meeting about fifteen minutes before actual meeting start time.

Use Log Out instead of Exit in the mobile app.

Please provide feedback regarding how Zoom works for PATACS meetings.

When asked whether there was an advantage of Zoom 1-to-1 meetings over Microsoft's Skype teleconferencing, Mel said there was not a lot of difference for 1-to-1. However, PATACS had problems hosting larger Skype meetings.

Stan Schretter gave the main presentation, "The Tablet Wars: Is there a clear winner?" Stan's talk focused on Apple iOS and Google Android tablets. Stan covered market trends for Apple and Samsung as the leader for Android and noted there is a "fight to the bottom" for the low-end of the tablet market. The Google Nexus 7 tablet was about half the price of the equivalent Apple iPad when released (July 2012), but now the price is about the same as Apple for an equivalent Android tablet. The recently announced Google Nexus 6 smartphone is the hottest selling item on Amazon before it became available (pre-order).

TechRadar.com Top 10 rankings list the Apple iPad Air at the top of all tablets (http://www.techradar.com/news/mobile-computing/tablets/10-best-tablet-pcs-in-the-world-today-1079603#articleContent). However, the Apple iPad Mini 2 is the best bargain.

The Google Nexus brand products are recommended for quick release of operating system updates. Other vendors may not upgrade the operating system as quickly, but Samsung is pretty good.

In a comparison of "Virtual Mobile Assistant" Apple Siri vs Google Now, Google Now provided more answers, but don't expect much! Stan preferred Google Now, which answers questions in the right way. Regarding screen size, Android tablets typically use the HDTV 16:9 aspect ratio. However, the new Google Nexus 9 is 4:3, the same aspect ratio that Apple used all along. Stan finds the 4:3 screen more convenient.

Internal storage is important. Stan finds 32GB (Nexus 9 maximum option, $479) is too little, and the Nexus 9 storage is not expandable. The Apple iPad Air 2 has 64 and 128 GB options. Stan also finds the Android hardware from HTC is really old.

When asked about Microsoft Windows tablets, Stan said that the Surface 3 Pro running Windows 8.1 is a wonderful device, but at $1,200 is $100 more expensive than the Apple MacBook Air.

Shopping on Amazon.com?
Remember PATACS!

If you shop online at Amazon.com, remember to start each session by clicking the Amazon link on the PATACS home page, then continue shopping on Amazon as usual. Doing so earns PATACS a 4 to 6.5% commission on your purchase at no additional cost to you.

Thank you for supporting your user group!

Help Wanted: Meeting Speakers

Look for the latest meeting information on the PATACS web site and in announcement e-mails. Finding presenters for our meeting programs is difficult—your help in the effort to enhance the value we all receive from PATACS membership would be greatly appreciated!

Please consider speaking to your friends at an Arlington or Fairfax meeting. We'd love to feature your take on a smart phone or tablet app. A presentation on these or other topics of interest to you would undoubtedly be welcomed by your PATACS colleagues. We have space in our schedule for 15, 30, 60 and 75 minute discussions—what are you waiting for?

We also have ready-made paragraphs you could use in e-mail communications to help us find speakers. Contact: director2(at)patacs.org

Linux and Open Source News
by Geof Goodrum

Potomac Area Technology and Computer Society
linux(at)patacs.org

Featured Open Source Software of the Month:
December 2014

The software described below can be downloaded at the links provided or copied onto a USB flash drive at the PATACS Fairfax meeting. However, please check the online package management tool included with your GNU/Linux distribution first, as installation is often just a click away.

Exo Platform – v4.1. http://www.exoplatform.com/. Free Affero GNU Public License, GNU Library or Lesser General Public License version 3.0 (LGPLv3) Java 7 code for Microsoft® Windows®, Apple® OS X® and GNU/Linux® by eXo Platform SAS. eXo Platform is the first cloud-ready enterprise portal and user experience platform-as-a-service (UXPaaS) for building and deploying transactional websites, managing web and social content and creating gadgets and dashboards. Built on open standards and open source technologies, eXo Platform has the features and extensibility of a UXP and the cloud architecture to build public and private clouds. eXo Platform features collaboration tools, user profiles, enterprise wiki, discussion forums, calendars, native apps for mobile devices, and much more. Minimum recommended system requirements include a multicore 2GHz processor, 4GB RAM, 10 GB disk space, and Java 7+.

**Stellarium** – v0.1.3.1. http://www.stellarium.org/en/. Free GNU General Public License source code and executables for Microsoft® Windows®, Apple® OS X®, and GNU/Linux® by Fabien Chéreau *et al*. Stellarium is a planetarium for your computer. It shows a realistic sky in 3D, just like what you see with the naked eye, binoculars or a telescope. It is being used in planetarium projectors. Just set your coordinates and go. Stellarium features a catalog of 600,000 stars by default with additional catalogs of 210 million stars, images of nebulae, constellation art, planets and their satellites, atmospheric effects, and a realistic milky way. Stellarium requires at least 256 MB of RAM, 150 MB of disk, and a OpenGL 2.1 3D capable graphics card

The Dark Mod – v2.02. http://www.thedarkmod.com/main/. Free GNU General Public License source code and executables for Microsoft® Windows®, Apple® OS X® (v1.08 only), and GNU/Linux® by Broken Glass Studios. Additional non-software content is under a free Creative Commons Attribution-Noncommercial-Share Alike 3.0 Unported license. The Dark Mod (TDM) is a first-person stealth game set in a 3D Gothic Steampunk world. The player controls an agile thief who must use his equipment and the environment to avoid guards, traps, creatures and other threats. There are over eighty downloadable missions and a campaign in development. TDM won PC Gamer's 2013 award for Mod of the Year. The TDM updater executable initially downloads 2 GB of base content and updates software for new releases. NOTE: 64-bit Linux PCs require 32-bit compatibility libraries.

Kernel Source – v3.17.2. http://www.kernel.org/. Free GNU General Public License source code for all platforms by the Linux community.

eXo Platform collaboration spaces
http://a.fsdn.com/con/app/proj/exo/screenshots/my-spaces.jpg
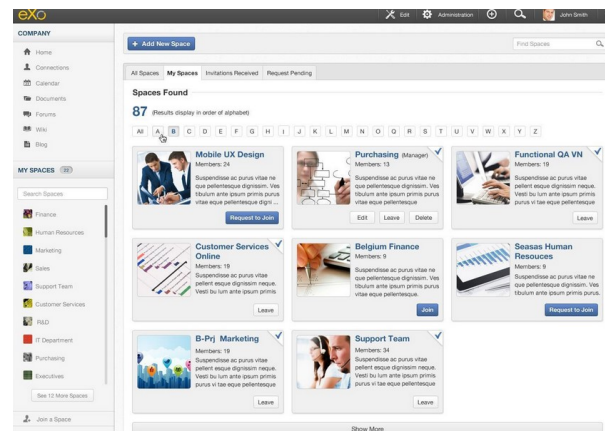
With All of the Media Reports About Massive Data Breaches, What Can We Do?
by Ira Wilsker

WEBSITES:

http://consumerist.com/2014/10/10/kmart-announces-credit-and-debit-card-breach-that-began-in-september/c

http://consumerist.com/2014/10/10/do-you-ever-shop-anywhere-congratulations-your-data-will-be-hacked/

http://www.usatoday.com/story/tech/2014/10/02/home-depot-data-breach-credit-card-fast-food/16435337/
https://www.annualcreditreport.com
http://www.verizonenterprise.com/DBIR/2014/

http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf
http://www.bloomberg.com/news/2014-10-10/sears-s-kmart-says-hackers-stole-payment-card-data-in-attack.html

http://www.kmart.com/en_us/dap/statement1010140.html

http://consumerist.com/2014/10/02/chase-data-breach-hit-76m-households-7m-businesses-account-info-not-stolen/

https://www.creditkarma.com

http://consumerist.com/2014/10/02/chase-data-breach-hit-76m-households-7m-businesses-account-info-not-stolen/

Tonight (October 12) on the CBS news magazine "60 Minutes" , the Director of the FBI, James B. Comey, discussed how the internet is a very dangerous place. Director Comey explained that because of the massive data breaches, the billions of dollars that can be illicitly accrued by cybercrooks and how it is often impossible to arrest and prosecute the villains because they are mostly in nations that will generally not cooperate with American law enforcement, that cybercrime on a massive scale is rampant.   The most likely source of the malware that has wreaked such havoc on our retail and banking industry has been Russia, where stolen credit and debit card information is readily and openly bought and sold. While most of the high profile data breaches and outright financial crimes are perpetrated against big businesses, it is almost always we the consumers who are actually being victimized.

Just this weekend (October 10), K-Mart acknowledged that its payment system had been compromised   (kmart.com/en_us/dap/statement1010140.html). In an official corporate press release, Alasdair James, President and Chief Member Officer of Kmart said, "I am reaching out to inform our loyal Kmart customers of a recent payment security incident. On Thursday, Oct. 9, 2014 our IT team detected that our Kmart store payment data system had been breached and immediately launched a full investigation working with a leading IT security firm. The security experts report that beginning in early September, the payment data systems at Kmart stores were purposely infected with a new form of malware (similar to a computer virus). This resulted in debit and credit card numbers being compromised." Later in the statement Mr. James stated, "There is also no evidence that kmart.com customers were impacted. ... I want our customers to be aware of the situation and I suggest that customers carefully review and monitor their credit and debit card account statements. If customers see any sign of suspicious activity, they should immediately contact their card issuer. More guidance is also available on our website, kmart.com and customers can contact our customer care center at 888-488-5978."

The advice presented by Mr. James that consumers need to carefully monitor credit and debit card statements for suspicious activities is sound, and is a repetition of the guidance previously offered by executives of other corporate victims of similar attacks.

According to an article published online at the "Consumerist" on October 10, the "top five" retailer credit and debit card thefts were the

2008 hack of Heartland Payment Systems where 130 million cards were compromised, followed by TJX Companies (2007, 94 million cards), Home Depot (2014, 56 million cards), Target (2013, 40 million cards and 110 million total records stolen), and CardSystems Solutions (2005, 40 million cards). While these data thefts from large retailers have garnered most of the publicity, again according to the Consumerist, there have also been millions of additional credit and debit cards compromised from smaller retail businesses, including recent breaches at Jimmy John's, Dairy Queen, P.F. Chang's, UPS, Albertsons, Jewel-Osco, ACME, Shaw's, Sally Beauty Supply, Goodwill, some Marriott hotels, Neiman Marcus, and Michael's craft stores. Most of the retailers that were recently compromised had their "POS" or "Point of Sale" systems compromised. Online financial services, as well as other companies with a strong online presence can also be compromised, such as the recent data breach at J.P. Morgan Chase in which personal and private data (but probably not credit and debit card information) from 76 million households and 7 million businesses was stolen, again probably by Russian hackers.

As we approach the peak shopping season of the year, many of us have some rational suspicions or fears about using our credit and debit cards at local and national businesses, as well as online. In the back of our minds may be the nagging doubt, "Will this card information be stolen?". In years past, there was a credible fear of a sales clerk or checker who might swipe our cards twice, once through the legitimate payment system, and then illicitly and immediately a second time through a simple device that reads and saves the magnetic st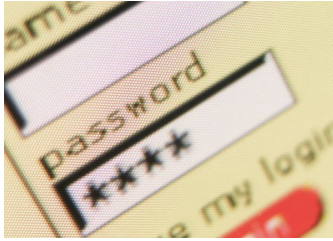ripe information. This allowed our information to be used by others for nefarious purposes. In last year's Target data theft, malware had been embedded into the payment system itself, such that even if we personally swiped our own cards at the checkout, with our cards never leaving our possession, our payment information was stolen at the instant that we swiped our own cards. International cyber crooks have found

used by others for nefarious purposes. In last year's Target data theft, malware had been embedded into the payment system itself, such that even if we personally swiped our own cards at the checkout, with our cards never leaving our possession, our payment information was stolen at the instant that we swiped our own cards. International cyber crooks have found that it is much more efficient and profitable to steal credit and debit card information by the millions through compromised payment systems, rather than the small numbers of local thieves stealing our information for predominantly local criminal purposes. These massive data breaches and hacks beg an answer to the rhetorical, "So what can we as individuals do about it?" According to the Consumerist, " Here's a cheerful thought: there is absolutely nothing that you can do about this situation. Individual consumers are pretty much powerless to prevent retail hacks." That does not mean that we as individuals are totally helpless, or that we must accept some degree of victimization. Certainly, there may be an increasing number of people who may prefer to pay with the traditional and anonymous cash, rather than digitally disclose private information, a sure way to prevent the information from that transaction from being used against us. Even though virtually all major credit and debit card companies offer a "no fraud guarantee" of some type, where the credit or debit card company will absorb any timely and properly reported unauthorized transactions, there is still a lot of aggravation and grief if the user is victimized, even if the losses will eventually be covered by the card issuer.

The Consumerist has several recommendations that we should all implement in order to minimize the threat, and to better recover if we are victimized by these cyber thieves. As has been mentioned many times previously in this column, for online purchases and financial transasctions, use complex randomized passwords, which should be changed periodically (many say at least every six months or even more frequently), and never use the same password on multi-

ple websites. Most financial websites offer and utilize a multi-factor authentication process, where in addition to a username and password, an additional security question must be answered, or a randomly selected term or number must be manually entered. When setting up these security questions, avoid using questions and answers that can be readily found on social networking websites (such as Facebook and Twitter), or other simple public information websites. Think about how many times you might have said something on a social network about your first car, favorite color, favorite flower, sibling's name, honeymoon location, favorite vacation spot, pet's name, and other information that could be readily used by others to complete your authentication sequence. Some of the more secure financial institutions actually select questions from old credit reports and other sources that unauthorized third parties will likely have easy access to, such as "what was your street address in the summer of 1983?"

While mostly localized, ATM and credit card skimmers are surprisingly common; these are devices placed by the thieves on the ATM or point of sale device, typically invisible to the casual user, that reads or skims a credit or debit card simultaneously as it is being scanned by the legitimate device. If using a PIN based card, such as a debit card, be sure to cover the keypad as you enter your PIN, preventing dishonest viewing by others, as tiny cameras are often placed with the illegal skimmer in order to read the PIN as the user enters it on the keypad.

Obviously, be very careful in reviewing monthly credit card and banking statements for

Obviously, be very careful in reviewing monthly credit card and banking statements for questionable transactions. Be cognizant that many fraudulent transaction are in small odd amounts, as they will be less likely to be noticed and questioned by the victim than large, round numbers. If anything questionable is found, contact the financial institution immediately.

It is not just credit and debit transactions that are being used to deprive us of our personal assets, but also other forms of credit and medical fraud. While there are commercials on TV touting a variety of credit reporting and credit score services, be aware that most of those, including some of those with the word "Free" prominently in their name, charge monthly or annual fees for the services that others may offer for free. The real source of free credit reports, as established by law, is Annual Credit Report dot Com (www.annualcreditreport.com), where each individual can get a legitimately free credit report from each of the three major credit reporting companies (Experian, TransUnion, Equifax), every 12 months. If any improper or unauthorized credit was extended, or erroneous data appears, instructions are provided in order to properly challenge questionable data. While not so much an indicator of fraud, many people like to monitor their credit scores, of which each of us have several different scores compiled for different purposes. Some credit card companies, such as Discover Card, now disclose credit scores directly on the monthly statement, as well as online, while an advertiser supported website, CreditKarma (creditkarma.com) offers free credit scores without ever asking for any form of payment.

Since the credit card companies are absorbing the massive losses from these frauds and scams, they are gradually implementing enhanced physical security directly on the credit and debit cards, such as embedded microprocessors, dual factor authentication, variable account numbers, and other technology that would otherwise make stolen credit and debit card data worthless. Since many of us will be doing a lot of our holiday shopping online, there is one tactic that may provide substantial protection form
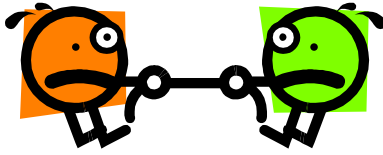
vide substantial protection form online credit card fraud. Most of the credit card companies offer a free service where the user can create some form of virtual wallet, where a unique, one time use credit card number is created for each transaction, and the user can often pre-determine a limit on each of these virtual accounts. Since the account numbers cannot be reused, they would be worthless to data thieves. Some of the new virtual wallets, such as those offered by Google and Apple, may allow us to utilize our mobile devices to make secure financial transactions, rather than by using a plastic

card. Some online payment services are offering a USB dongle that creates a new unique account number every few seconds, making previous account numbers obsolete as the new numbers are created.

Inevitably, this will be a classical "cat-and-mouse" game; as new security devices and methods are created, the cyber crooks will find a way or method to defeat them. This is a win. Our financial health is at stake.
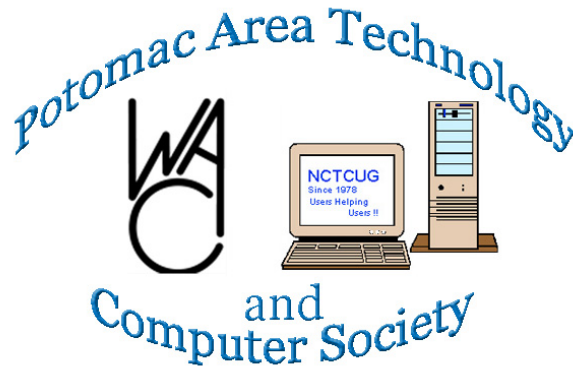
~Potomac Area Technology and Computer Society, Inc.~
~ A Non-Profit Membership Organization Serving Personal Computer Users and Technology Enthusiasts ~
~ in the Washington, DC Metropolitan Area Since 1978 - Three Monthly Meetings in Northern Virginia~

And You Offer Me What???

Valuable Information From The PATACS Site

And now - YOUR TURN

What resources do you recommend?!?

Our site, patacs.org, has much valuable information - worth taking your time to discover. Also, you can offer suggestions on additional topics or articles. You will find vendors recommended by members. Vendors of goods and services are not endorsed by PATACS, or its members, but have been found by members and friends to provide good value, prompt service, or offer unique products.

O'Reilly Media - Books, eBooks, Technology, conferences. **User Group Members receive 40% discount on print books, 50% discount on eBooks in many DRM-free formats.** O'Reilly has been providing books and ebooks used by PATACS for door prizes and "thank you" gifts for presenters. Lines include O'Reilly, Pragmatic, No Starch, Rocky Nook, and SitePoint products. Also eBooks from Wiley, Wrox, Sybex, Visual, and For Dummies. Store **Link**. Use discount code: DSUG

Buy.com - Computers, software, books, music, other tech products. Items frequently get free shipping, and with stocking locations in PA, packages arrive in one or two days with lowest cost shipping. Good for multi-seat paks of security (AV, Firewall) software, often difficult to find in retail stores. "I've bought software and OEM laser print cartridges from Buy.com since 1998, and have been very pleased with pricing and quick receipt of orders." - P. Howard

Print Pal Printer inkjet cartridges, laser toner cartridges. Recommended by Dean Mires for quality refills.

Batteries Plus - Retail locations locally: Rockville, Fairfax, Chantilly, Woodbridge. Carry large assortment of batteries (UPS, Lantern, flat cells, household) and light bulbs. Recommended by Paul Howard. They will make up custom batteries from cells, for tools, electronics, while you wait, or for later pickup.

Battery Mart - web vendor, locations in Winchester, VA and Martinsburg, WV. Recommended by Roger Fujii for UPS batteries. "I ordered 2 UPS batteries and packages of AA and AAA cells on a Sunday evening, received Tuesday." - P.Howard

703-516-0300, Custom builds, parts & accessories, tech support (Screwdriver Shop). Recommended by Gabe Goldberg. PATACS Meeting Presenter, April 2014.

TCS Computer, 703-913-0900, Abi Soltani, Systems Engineer - Custom system builds, parts and accessories, tech support. (Screwdriver Shop) Recommended by Jorn Dakin. Presenter, April 2014.

Stevenson On-Site Repair Service (540) 439-2999 They're honest, economical, knowledgeable, friendly, reliable! From their website: Repairs Laser Printers, Fax Machines, and Printing Equipment. Specializes in helping maintain Hewlett Packard, IBM, Okidata, Brother, and other quality laser printers. In business since January, 1991. Recommended by Gabe Goldberg.

PATACS Annual Financial Report, Fiscal Year 2014
By Paul Howard, Treasurer

PATACS's fiscal year concluded on September 30th. Although we experienced a negative cash flow of $1377.23, the group is in excellent financial condition. Results from Operations reflect $2386.68 in expenditures to replace a 10 year old video projector, acquire a wireless mic system, audio mixer, cables, surge protectors, and other costs to enhance Arlington meetings.

Donations are vital to the fiscal soundness of the group. Member generosity accounted for 33 percent of our income. These donations received were $106 more than in FY 2013. Amazon commissions via our website links were $471.46

Member donations were received this year from: Goldfarb, Graham, Harvey, Housley, Howard, Lusby, K. Johnson, M. Johnson, Leggett, Loew, Mabudian, Mikosinski, Porter, Schmidt, Scheuman, Smith, Throneburg, Weeks, Wertime, Willard, and Vestrich.

Pizza SIGs were sponsored by Jim Brueggeman and Jon Mabudian, who picked up the entire check for a meal session, while the attendees donated the amount of their bill to the club. Pizza SIG donors include Brueggeman, Chance-Sampson, Fraser, Fujii, Garson, Goldberg, Howard, K. Johnson, Mabudian, Mikosinski, Schmidt, Throneburg, Walsh, and Wenri.

PATACS is financially sound because of prudent planning and fiscal restraint. Membership stands at 100. Our "rainy day fund" was established many years ago, and is held in interest-bearing accounts. Interest yields on insured deposits are disappointing, but will continue until the Fed changes its low interest rate policies.

Our reconciled account balances within our Quicken accounting system at the close of the fiscal year (September 30th) were: Checking Account $4461.22; Interest Checking - $11,569.68; CD account: $1110.09.

During the year, the Financial Oversight Committee has been working on methods to improve the efficiency of our biennial audits. Documentation on the Society's Financial System has been revised to reflect current practices, and is available on the website. A four-page document describing the Treasurer's procedures has been prepared.

This Annual Treasurer's Financial Report for Fiscal Year 2014 has been approved by the Board of Directors of PATACS on 10/20/2014. The account balances noted above are based on on-line and email queries of our banks – statements for all accounts as of the 9/30/2014 close of the fiscal year have not yet been received. On that basis, the balances and the Cash Flow Report below are certified as correct.
Paul Howard, Treasurer   James Rhodes, President

The "organizational documents" area of our web site contains additional information about the user group's financial operations, including prior years' Financial Reports for comparison purposes

PATACS Cash Flow Report
FY '14: 10/1/13 - 9/30/14

Revenues

Pizza SIG Cash Donations	806.00
Donations by Check	655.00
Total Donations	**$1461.00**
Membership Dues	**2425.00**
Interest Income	**13.45**
Amazon Commissions	**471.46**
Total Revenues	**$4370.91**

Expenses

Insurance - Liability & Personal Prop.	425.00
Legal - VA Corporation Fee	25.00
APCUG Dues, Editor Recognition	214.33
Donation – Friends of OLLI	250.00
Total Administrative	**$914.33**
M'bership / PR – Printing, Hospitality	**$139.35**
Door Prizes	61.47
Meeting Hall Expenses	24.34
Webinar Services Expenses	353.52
Meeting Equipment	2386.68
Total Meetings & Other Svcs	**$2826.01**
Newsletter Assembly	102.35
Newsletter Postage	558.03
Newsletter Printing	968.16
Total Newsletter	**$1628.54**
Web Site – Domain / Hosting	**$239.91**
Total Expenses	**$5748.14**
Results from Operations (Loss)	**($1377.23)**

Prepared 10/20/2014

PATACS Information

PATACS, Inc. 201 S. Kensington St. Arlington VA 22204-1141

Club Information call: 703-370-7649   **Web Site: www.patacs.org**

Posts is an official publication of the Potomac Area Technology and Computer Society (PATACS), a Virginia membership corporation. PATACS is a tax exempt organization under section 501(c)(3) of the Internal Revenue Code. Contributions are gratefully received and tax deductible.

Posts provides news, commentary and product information to PATACS members. Products or brand names mentioned may be trademeakes or registered trademarks of their respective owners. The contents of articles herein are the responsibility of the authors and do not necessarily represent PATACS, the Board of Directors, nor its members.

E-mail article submissions and reprint requests to editor(at)patacs.org

Membership Policy

Membership dues are $25.00 (U.S.Funds) per year, with a $15 surcharge for international mail. Membership in PATACS includes membership in all SIGs, access to the software libraries, and subscription to the Posts published 12 times per year in print by US Mail and PDF download by Internet. Applications may be obtained at any club meeting, by downloading from the website, by calling one of the officers or board members, or by writing to the club. A sample newsletter, membership application and related information may be obtained by enclosing $2 (for US addresses only) and mailing your request to the membership address. Please do not send cash by mail. Payment and applications may also be submitted at any meeting, or mail to: PATACS Membership, 4628 Valerie CT, Annandale VA 22003-3940

Advertisement Policy

Members' advertisements: Ads are accepted from members for non-commercial purposes at no charge. Copy should be sent to the Editor in the same format as article submissions. Commercial Advertisements: Ads are accepted from commercial advertisers at the rate of $40 per full page, per appearance, with discounts for multiple insertions. Smaller ads are priced accordingly. Payment for ads must be made in advance of appearance. Advertisers must supply a permanent address and telephone number to the editor.

Reprint Policy

Permission to reprint articles from the PATACS Posts is given to school, personal computer club, and nonprofit organization publications, provided that: (a) PATACS Inc. receives a copy of the publication; (b) credit is given to the PATACS Posts as the source; (c) the original author is given full credit; and (d) the article author has not expressly copyrighted the article. Recognition is one means of compensating our valued contributors

If you are moving

Please send your change of address to the club address as soon as possible to avoid missing issues.

Thank You!

Upcoming Meetings

PATACS Arlington -

(12/3) 7 PM: General Meeting

Board of Directors - (12/15) Arlington

None in December: Technology and PC Help Desk

OPCUG / PATACS - **(12/13) 1 PM**, Fairfax - OLLI Tallwood

"Virtual Roots" - Genealogy; Presented by Sharon MacInnes

Learn 30: TBA

Microcenter Clinics

See http://microcenter.com/site/stores/ instore-clinics.aspx

for the latest new9s on these free clinics.

PATACS Meeting Information

Call (703) 370-7649 for meeting announcements

Scan the QR code at left or enter

http://www.patacs.org

to visit our web site

Free Admission — Bring a Friend!

Arlington Meetings

Carlin Hall Community Center
5711 S. 4th Street, Arlington, VA 22204
http://www.patacs.org/arlingtonmeetings.html

General Meeting
1st Wednesday, (12/3), 7 pm

Technology and PC Help Desk (SIG)
None in December

Board of Directors
3rd Monday, (12/15), 7 pm

Fairfax Meetings (with OLLI PC User Group)

Osher Lifelong Learning Institute (OLLI)
4210 Roberts Road, Fairfax VA 22032
http://www.patacs.org/fairfaxmeetings.html

General Meeting
3rd Saturday, (12/13), 1 pm

Online-Only Webinar
2nd Wednesday,(12/10), 7-9pm
http://www.patacs.org/webinarpat.html