Academic Paper

Dyamonte Mizell

4/21/23

CPD 494

Instructor Porcher

E-transactions are getting harder and harder to conduct safely now that they have been around for some time.

Society as whole is thankful for E-transactions because it allows for them to use their wallet easier. The transactions include ApplePay, SamsungPay and more. These web transactions are not as safe as everyone thinks they are. The problem lies within E-transactions and their lack of security when it comes to addressing hackers, malware and data stealing. E-transactions mostly use mobile wallets when it comes to purchasing services and products. This improved innovation created by a group of entrepreneurs will improve mobile wallets through protection, satisfaction, and service. There are many problems to address when it comes to mobile wallets. This includes identity theft, device spoofing, and velocity attacks. Device spoofing is when a hacker attacks a certain device and steals all the info off the device and stores it on a device that they own. The hacker can spoof your device and now have all access to an individual's mobile wallet. When discussing identity theft, this is a lurker who stalks your payment, pay stubs, and other economic dealings and under your nose they steal your identity. This means that they have access to your bank , credit cards, health info, and more. This is where our E-wallet with our special built in protection card steps in. Our built in protection card has firewall security that is specifically designed to block attacks such as identity theft and spoofing of a device. The firewall security prevents malicious attacks that could be trying to go through two-factor authentication, card skimmers, and more. There are velocity attacks. In which lies another problem with mobile wallets, velocity attacks occur when a fraud has stolen your information from your card and keeps making unauthorized purchases until the card number is verified. There is a well enough complaint list of problems with e-wallets yet any innovator has been thought to solve. Until today with this innovation of an e-wallet with a built in protection card.

With our built in card protection there is no need to worry about velocity attacks because our card will have biometric authentication. Our biometric authentication is built-in to the card of our e-wallet and is used with face authentication or fingerprint. This was designed to limit the stealing of information from bank cards. Bank cards don’t have any protection if they are stolen, lost, or disabled. Our built in protection covers all of that so the customer doesn't have to worry about that anymore. Even if your card is stolen or the information from your card is stolen the perpetrator won’t be able to use it without biometric authentication. So if they don't have your fingerprint or face scan the card is unusable. We designed this because of how people used to complain about mobile wallets having their card info stolen. There wasn’t enough security for mobile wallets before we stepped in with our innovation. This innovation was designed to solve all the problems that were brought up when discussing mobile wallets. The people want to not worry about identity theft, malicious attacks, and spoofing when they open their mobile wallets. The world of technology is forever growing and mobile wallets before were not enough to keep up. Our E-wallets with built in protection card is the next innovation to take the world by storm. This innovation will have a major impact on technology and what the future of e-wallets will look like. This e-wallet was built for the sole purpose of protection . I would suggest better protection but mobile wallets had little to know protection, the only aspect that could be accounted for was two-factor authentication. Two factor authentication is very commonly easily bypassed by amateur hackers. Our e-wallets are going full force with security management plans to advance mobile wallets and provide great service to users who won't have to worry about those security risks.

The problem at hand is that chip card readers are very easy to attack and hack so we made a solution to solve that problem exactly. According to the journal “Chip Card Security”, “because of the change in credit card security, banks are phasing out magnetic strip cards in favor of more secure authenticated ways to pay”(Zumber, 2015). This is why we started this innovation as a group, to have a stronger security card that attackers can’t just bypass when they feel like. The journal states “EMV cards are designed to prevent fraudulent transactions when someone swipes a counterfeit card at a payment terminal”(Zumber, 2015). The EMV card is similar to our card innovation but less stronger. There have been cards in the past designed to help stop fraud from going on but nothing has cracked the seal a 100% as of now. This is why our innovation has stepped up to take the role against fraudsters who want to gain control of people's cards, money, and information. We are here to give solution based cards with built in protection to fight against those who want to attack. We came up with strong firewall security plans in order to prepare for those who try to engage in hacking information from our innovation of e-wallets. They might have done whatever they wanted with regular mobile wallets but they are going to have to come a lot harder than that if they want to stand a chance. The article stresses the importance of chip card security and that's our main priority when it comes to this innovation. The security of the user's card is the main goal of this project. After all there is know product on the market that is accomplishing this as of right now. We need more security in order to protect users in a way that they actually feel safe. The problem is attackers having their way with stealing chip cards information. They're red hot right now and even the legal system can barely stop them. With our new built in protection card from our e-wallet there will be change and I can guarantee that. No more will hacks just do what they want and however they want. They will face a threat they have never seen before, even EMV cards are not enough. We created something as entrepreneurs that is more than enough to outlast these hackers.

Secondly we have the article “Determining Factors of m-wallets adoption”. This article discussed how m-wallets are more valuable than cash. The article stated that “M-wallets are more advantageous and convenient than carrying cash around”(Reham, 2022). I do agree with this take and this goes to our point of being innovators as well. While m-wallets are all good they have little to know protection. There is an upgrade from cash but not too much. This is why our e-wallet with the built in card protection will be a great standard for people to use and feel secure. The article findings revealed that “confirm the significant effects of privacy concerns over the consumers’ intention-to-use m-wallets i.e. perceived security”(Reham, 2022). This is true that privacy concerns of users who use the mobile wallet happen often. The reason for this is because many people have seen that even m-wallets can be hacked into and their information can be stolen as well. They think that people might as well just use cash and their physical wallet if their information is at risk using an m-wallet. The great solution we have to this problem is our e-wallet. Our e-wallets get rid of all these worries from users and put them at eaze. Our invention is ten times the security that a m-wallet has and significantly easier to process. We have the security systems on our innovation beefed up to handle the pressure. When the community needed a better service for mobile wallets , we came to the rescue. There is more to our e-wallet than a regular m-wallet, that a normal person could barely process the thought of. We want to expand our innovation to get rid of hacking worries and this is why the e-wallet was created in the first place.

They are barriers when it comes to mobile wallets though and that's a tough break. This scholarly journal titled “Barriers towards the adoption of mobile payment services” discusses the faults of mobile wallets. The lack of security with mobile wallets is the problem that everyone is concerned about. The usage barrier is what was discussed in the journal and it means that m-wallets are an advanced technology that is expired. The journal states “Innovations require consumers to change as new skills need to be learned and existing habitats need to be modified to be able to use a new product or service”(Haiss, 2017). This means while the m-wallet was a great technology , hackers have caught on to its system networks and can break it in easily. The m-wallet system needs to be modified and given an upgrade in order to stand a chance against attackers. This is where the innovation of the e-wallet steps in and makes improvements. The journal states “If the new product or service implies higher efforts for consumers, it is likely that it will face resistance”(Haiss, 2017). The service of the e-wallet will have high success rates when it comes to facing resistance against attackers. The perfect candidate to imply higher efforts to consumers is no other than the e-wallet. The e-wallet is designed to have improved security over the m-wallet. The consumers want improved methods and efforts, which the e-wallet has improved methods such as, detecting chip skimmers. This is one of the best selling points of the service. Mobile wallets have to now way of protecting their service from card skimmers. Card skimmers can be a problem designed to read chip cards and steal information through the card reader. It’s supposed to be a trick for attackers to steal your information without you noticing a thing. The built in card has a firewall system feature in the chip part of the card that can block the attacks from the skimmer. This will be a great improvement that all the consumers were looking for and they will be glad that this was offered through e-wallets. The journal was implying there was a need for improvement on the mobile wallet because of its barriers but the e-wallets eliminates all these barriers with eaze.

One of the factors that made the innovation of the e-wallet come to light was the problem of identity theft. The crime has been increasing yearly with looks to be no stoppage soon. The scholarly article named " The Impacts of Facilitating and Inhibiting Factors on Usage Intention of Mobile Payment Services", discussed the problems of the mobile wallet that hold customers from using it. One of the key factors was the fear of financial loss voted for by consumers. One way that financial loss can come abroad is hacer taking an identity that isn't theirs and using all the information maliciously. Identity theft deals switch loss of money, access to accounts, and more. This is a good enough worry of a problem for consumers to take concern in this matter. The journal states "Moreover, perceived risk had a significant negative impact on usage intention, with the greatest impact from the factor of financial risk"(Chen ,2020). This means that consumers don't want to take the risk of getting an e-wallet because of the implications that come with it. The risk is not worth the reward to consumers but we give them a reason to with our e-wallet. We will give the consumers what they want with better protection and better network security systems. Customers will not have to worry about identity theft when dealing with e-wallets because of the biometric authentication feature. When the hackers want to steal your information, they first go through the password of your accounts. Now typical consumer passwords are not hard to bypass at all especially if it's two factor authentication we are dealing with. This means we need something greater than two factor authentication when it comes to mobile wallets. The e-wallet advances the problem of two factor authentication by providing authentication that requires some form of fingerprint or facial recognition.

Keeping on the thought of identity theft, there was another journal that put their spin on this topic. This journal titled “Analyzing of e-commerce user behavior to detect identity theft” was a discussion of creating survey data that used different factors in order to detect identity theft. The journal states that “System which is the most prone to identity theft is the e-commerce system since the system is growing rapidly” (Vuckovic et al., 2018). This is true as the e-commerce stupid grows the more people that use mobile wallets increase as well. This comes with a negative clause though as many of the people are subject to identity theft with the increasing of the e-commerce system. The journal states “the market views the investment in anti-identity theft as a tool to enhance competitive advantage and firms should be encouraged to adopt identity theft countermeasures more proactively” (Vuckovic et al., 2018) . This means the service market is setting a standard for mobile and e-wallets to create methods to combat identity theft. The market wants the best service for consumers to not worry about identity theft. This is where e-wallets come in with having behavior trackers installed into the card. If the card notices unusual behavior trying to be used then the card will shut down and need to be reinstalled only by call in appointment for confirmation to business headquarters. This will prevent those who are trying to steal identities as they will already set off our firewall systems with suspicious activity so that will let us as a service to watch for activity. If the attacker somehow gets past the firewall then the card will automatically shut down and that will let us know if someone is trying to steal someone's identity or pull a malicious attack. E-wallets are fully fledged prepared to handle identity theft attacks no matter what.

The unspoken part of e-commerce is the transition of cashless payments, having cashless payments may be a bigger problem than you think. The scholarly article titled “The effect of cashless payments on the internet and mobile banking” is a discussion of the impact of cashless payments when it comes to usage of mobile banking. The journal stated ”Based on the DOI theory, discovered that promoting the features and advantages of e-wallets, as well as ensuring the compatibility”(Chong, 2022). The problem at first with cashless payments was that they didn't provide enough coverage, this led to mobile wallets not having enough to protect against e-commerce attack interactions. Then the e-wallet came about and changed the game. As the article stated, promotion of features wins over customers from the risk that they think they are facing. If we keep promoting the innovation built in protection features then we see a great customer surge in the future. The e-wallet is here to solve cashless problems such as velocity attacks. Velocity attacks are used without cash but instead credit or debit cards. These attacks can be spammed until they hit on a singular purchase, all they need is one purchase to go through in order to gain satisfaction. With e-wallets they won’t gain any satisfaction as security programs with different channels in order to gauge this problem. Our multiple security teams are on standby in order to have a great stance on these cashless payments and make sure that everything is in order. If the security team notices word or unusual behavior with a users built in protection card then the security teams will follow procedure and ultimately shut the card down and alert the user of this activity.

While you can go down a list of how many problems come with in the world of virtual wallets you can’t argue when an innovation is coming up with procedures to eliminate the problems. The scholarly article titled “Virtual Wallets, real complaints”, is one deep dive into all the possible problems that came with a mobile wallet. The article stated that “The three most commonly complained-about issues involving digital wallets are problems managing, opening or closing accounts; problems with fraud or scams; and problems with transactions (Mierzwinski ,2021). Those are three major problems that come with mobile banking and this is what the consumers have the most to debate about. I would say fraud is one of the biggest ones to worry about because once the fraud has come about it's hard for customers to gain back their account how it was left. This is why e-wallets strive the hardest to prevent fraud baking with the built in credit card. This is why the e-wallets team up with banks and share fraud data reports in order to learn how to combat this action. With the bank and e-wallets both on the same page there is no way fraud attacks can stand a chance against the built in protection card. The data reports will let us engage and analyze how the fraudsters are moving, meaning how fast, effective and damaging their attacks are. If we catch a break such as a pattern we can use that to combat the fraud attacks and get the upper hand against them. This team up will solve the problem of both banks and e-wallets being attacked at a high rate with no solution as both both heads combined can have the best of security teams working behind the scenes to manage thes fraud attacks. This will allow us to expand our innovation to heights never seen before by a regular mobile wallet or mobile banking. Enhancement is the key to the innovation of the e-wallet.

We discussed how this innovation and problem relate to classes taken outside my major even though it is highly attached to it. My major is cyber security and our innovation of e-wallets ties in heavily into the cybersecurity aspect of things. I will start off with criminology classes that I have taken in the past. These classes are connected to a criminology major but they also tie in with our innovation. This first thing to bring up is that the reason we created this is because criminals are at their peak when it comes to stealing information. In my CRJS 310, we often talk about frauds, hackers, and attackers. All of these problems are the reason we created our innovation. Criminals who are subject to do these acts of stealing info which we discussed in my criminology class. They are various slideshows from the module material of my criminology class that present reasons why security is lacking when it comes to mobile wallets. One of the reasons was methods of authentication, which I had mentioned earlier about mobile wallets. They need better protection than two factor authentication and it’s simply not enough. We also discussed biometric authentication which is stronger than two factor authentication. This is what we will use for our innovation. Biometric authentication with e-wallets will change the game as we know it. Hackers will be far behind and not expect this change which will lead to less security mishaves. Hackers can steal credit card info, card numbers, payment stubs, and more. The fingerprint or facial recognition is the one thing these hackers can steal from users. This is why I suggest our innovation will be better than any mobile wallet before. WE saw the problem of easy access authentication and came up with a way harder way for hackers to just get access to your information. It won't be as easy as it once was with mobile wallets and this will serve as a shocker to those hackers. To the users who use our innovation this will be a dream and a load off of their back.

I had a communications class called COMM 372T that dealt with new media technologies. In this class the material modules discuss how people can be easily influenced over social media. One of the problems we had with mobile wallets was spoofing. In today's age, hackers are getting smarter daily with their ideas to steal information from users. They will even use social media. In this class, we discussed scammers in an online setting. The correlation is that scammers are connected to spoofing and on today's internet social media is the best way to spoof. Hacker will send you direct messages on Instagram,Twitter, and Facebook and any other media platform to gain information. Hints the name spoofing, with little to no protection it is easy for hackers to get your info if they're pretending to be your friend on social media. If they want your bank information from your mobile wallet they will scam you con artist style by telling them to give your information up and they will pay you a good amount of money which we learned in communication class. With our biometric authentication, you could give the hacker on social media all your info and they still wouldn't be able to get into your info. With a regular mobile wallet they would but not with our e-wallet with built in card protection. Our e-wallet won't fold, bend, or break when hackers try to persuade you with their scamming tactics. We have made sure of that by giving you the option to use face scan or fingerprint as your means to access your card. Access to a user card is exactly what the hackers want and we decided to solve that problem and block them from getting it at all. They're going to have to try harder than ever before in order to gain access to a user's card with the biometric system we have in place for the e-wallet.

To determine if our innovation is effective we can put it through the trial of hackers trying to get access to the mobile wallets versus e-wallets. We can have timers set up to see if the hackers get into which version of mobile wallets first. The regular mobile wallets will be up against our e-wallet with a built in protection card. The regular bank card will not be as effective as the built in protection card for security purposes. We can also test our firewall protection, after our innovation is done with test trials. We can test the security breach for the by running our own security test scan to determine if the built in protection card will fall under malicious attacks. Basically we will do trial and error test runs on our e-wallets versus a mobile wallet to see who functions the best when we have an attack underway. If our functions succeed then we will know it is effective. The first check off is seeing if an attacker can steal information from the e-wallet. Our main goal is that information cannot be stolen because they need to get through the biometric authentication first in order to steal a user's information. Once the attacker tries to get past the biometric authentication and fails because they can’t steal the user face scan or fingerprint we will then know our product is successful. We also can determine the product is effective by using the card in a card skimmer. Card skimmer is another form of fraud, Examples include inserting your card into a 7/11 card reader and stealing your information from under your nose. This is a sneaky attack for malicious reasons to steal your information from your card and use it for their own gain. We can put our built in protection card up against the card skimmer to see how effective the card is. As entrepreneurs we looked out for the users who don’t know about this information and put firewall protection systems surrounding the card which do not let us down when it comes to a card skimmer. Card skimmers usually work on unprotected cards but with our protected card it won’t even stand a chance. Regular mobile wallets don’t have this type of protection to be as effective as our e-wallet.

Because of the technology based innovation we have discussed, we need extensive equipment in order to get this project up and running. In order to get this innovation turned into reality we need to get a processing card that allows multiple forms of payments. The card will be used as our brand, an example of this like the cash app card. Our own designed card is the built in protection card under our brand and will have apple pay, samsung pay, venmo and more options available. Next we need a system that allows for our e-wallets to be processed on. The system we will use is near field communication. This allows for two devices to exchange information. The NFC communication will allow the use of apple pay or mobile pay for the card. Then there is Magnetic Secure Transmission which is a magnetic signal that the built in protection card will have so the card reader can read the card. There will also be QR codes on the card that transfer to the mobile device so that it can be scanned for payments. The QR code will be in place for the e-wallet so that it can be scanned at places that allow scanning for QR codes. We will then need a firewall protection system in order for protection of the e-wallet. The firewall protection system does the job of making sure data coming from the internet is verfired safe. We need this in order to make sure when the e-wallet has transactions that every transaction is safe and secure. In order to get the firewall we can choose between companies that offer this service. The service we will choose is software-based firewall. This will allow us to have a host service for the security of the firewall.

Next we will need the users help in order to form the biometric authentication. Users will have to agree to privacy terms and agreements in order for the biometric system to work. Biometric authentication uses the biological features of users so we need their approval of use before the innovation can use it. Once they agree to the use of their biometric features, the system will store the information in order to verify the user's identity when they want to access their account. Next the e-wallet team will need a veteran security team that has previous work with blocking hackers, malicious attacks, and spoofing. This security team will be able to go over plans in order to manage attacks, and rescue plans for users. We want our users to be safe, and a well experienced team of cybersecurity specialists will get the job done forsure. We also need partnerships with banks in order for the security team to work with them and share data reports. The sharing of data reports will allow both us as innovators and the banks in partnership to get ahead of attacks and be more advanced than hackers. Both teams will benefit highly from this and the users of either the e-wallet or bank cards will be secure . Then will need a service that detects chip skimmers. This is one the hardest parts because chip skimming is one of the hardest attacks to catch before it’s too late. This is why we get a protector for the chip in the card that automatically comes with the e-wallet. There will be no need for a user to go out of their way to purchase this because it is automatically built in the card that the e-wallet uses. The final aspect we need for this innovation is customers. For every product or service, you need customers. There is no doubt that once the innovation was to hit the market that we would have consumers. Once we get the customers on our side then the e-wallet with built in card protection will all set to go.

The next steps will be to get this service on the market for consumers to use. This means going through the typical business standards and making sure the entrepreneurs get an LLC and all that important aspects of creating a product or service. What I have learned from this project is that working with a group takes more work than working alone. Working with a group is an effort and you can slip up but someone in the group can pick you up. I learned from my group members more information than I knew before. Before the project I didn't think creating a mobile wallet would be as difficult but there are a bunch of tiny aspects that go into a little card. This card needs protection, modification, and technology advancements in order to actually work. There is more than meets the eye in order for this card to be successful. I applaud the creators of the mobile wallet because I know it took time to get this idea to life. We as entrepreneurs wanted to advance the mobile wallet with the e-wallet so we had a lot on our plate as well. Things that I would have done differently is have more in person discussion with my group, then I would have felt the group experience more. We had various zoom calls but I feel as if we could have done in person more. We could have had ideas that went smoother and were more advanced. Our ideas now are great and surpass the mobile wallets now as well though, not taking anything away from the e-wallet. I also learned that being an entrepreneur has to be the top five hardest jobs in the world. This is no easy task at all and not everyone can be a great entrepreneur, there is more to it than people think.

References

Chen W. (2020.) "*The Impacts of Facilitating and Inhibiting Factors on Usage Intention of Mobile Payment Services"* . International Journal of Applied Science and Engineering. https://gigvvy.org/journals/ijase/articles/ijase-202003-17-1-107.pdf

Chong L. (2022). "*The effect of cashless payments on the internet and mobile banking".* National Library of Med. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8897554/

Haiss F. (2017). *"Barriers towards the adoption of mobile payment services"*. Karlstad Business School. https://www.diva-portal.org/smash/get/diva2:1114478/FULLTEXT02.pdf

Mierzwinski E. (2021) "*Virtual wallets, real complaints"* . U.S. Pirg Education Fund. https://pirg.org/edfund/resources/virtual-wallets-real-complaints/#:~:text=The%20three%20 most%20 common%20 complain

Reham M. (2022). "*Determining the factors of m-wallets adoption*". Plos One Journals. https://doi.org/10.1371/journal.pone.0262954

Vuckovic Z. (2018). "*Analyzing e-commerce user behavior to detect identity theft*" . Statistical Mechanics and its Applications. Retrieved 24 May 2018. https://doi.org/10.1016/j.physa.2018.07.059

Zumber R. "*Chip Card Security: Why Is EMV More Secure?*" . The Bottom Line Journal. https://squareup.org/us/en/the-bottom-line/managing-your-finances/why-are-chip-cards-more-secure-than-magnetic-stripe-cards