How do we bring E-transactions to the physical world while making them more secure and accessible to conduct?

Logan Powell

Old Dominion University

CPD 494

Professor Porcher

4/21/2023

How do we bring E-transactions to the physical world while making them more secure and accessible to conduct?

As the digital world continues to grow and become more prevalent in our lives, the growing threat of attacks and possible loss of information also grows at a steady rate. More countries are adapting to using e-commerce as an alternative form of payment for all types of expenses from everyday items such as groceries to growing small businesses, to paying fines and bills. The age of digital currency is upon us, and will only continue to consume the paper money industry as we come to discover more in the realm of possibilities in the cyber domain. The question here to answer is, how do we go about bridging the gap between these two worlds? How do we connect the two industries while maintaining safety and effectiveness that is future proof for the ever changing business? ***How do we bring E-transactions to the physical world while making them more secure and accessible to conduct?***

To accomplish the task of understanding how to do so, the group decided to address the problem of how to bring electronic transactions into the physical world by making them safer and easier to execute. We decided that the best way to do this is to create a mobile wallet. We wanted to make our mobile wallet universal so you don't have to use specific devices or choose providers like Apple Pay.

In order to use Apple Pay, you first need an Apple device. Another thing it requires is a merchant that accepts Apple Pay. The third requirement is a secure connection between the payment system and the reader with excellent encryption to protect your data. The last thing it needs is a user willing to adopt this technology. The same can be said about competitors such as Google Pay, Samsung Pay, Android Pay, etc.

Our team aims to target those users who do not want to be locked into a hardware ecosystem, vendors who want to bring customers from all these ecosystems instead of choosing between vendors and removing the required technology component. Our innovation is a physical card mobile wallet that allows you to pay from any of these ecosystems anywhere credit card or mobile payments are accepted. It also converts currencies for you so you can use bitcoins in physical stores or online stores for free. That way, you can travel without having to worry about bank opening hours and rules that apply abroad.

Currently, the e-commerce world is very open to all. There are little to no limitations to the cyber domain, meaning the same for e-commerce. With the use of certain tools available to almost anyone via the internet, anyone can become a cyber criminal capable of stealing information, accessing sensitive documents, and gaining access to restricted domains. One of the largest reasons this is so prevalent is due to the difficulty in trying to catch some of these cyber criminals. As stated earlier, with the use of certain tools both paid and unpaid, the possibilities are endless when it comes to trying to track down an individual from a single digital footprint they left behind. Being anonymous within the cyber domain can be an easy way to hide for those that are aware of what they're doing. These criminals then can attempt to attack almost from a risk free position in which they are put at minimal danger to their well-being, while inflicting massive damage to an individual or business.

While attacking may sound like an easy task, for those who are unaware it can be even riskier due to the possibility of mistakes, as well as not having the experience to conduct such an operation. These criminals conduct all sorts of attacks, some being physical and some via the the digital world ranging from identity theft acquiring sensitive information, to brute force velocity

attacks, to using spoofers to impersonate an individual in hopes of gaining access to special accounts, to lastly skimming peoples cards at gas station pumps and card readers.

The integration of e-transactions with physical transactions poses a few challenges. One of the main challenges is secure verification. When conducting an e-transaction, consumers can verify themselves by adding a password, fingerprint, or other biometric degree. Be that as it may, when conducting a physical exchange, customers frequently depend on credit cards or cash, which are vulnerable to theft. Subsequently, there's a need to create secure verification strategies that can be utilized in both e-transactions and physical exchanges.

Being cyber security majors, the main concern of the product was to ensure that this product is safe and protects consumers from data theft. According to Pymnts.com: "Consumers do not feel secure when using a mobile wallet and prefer to use physical cards. This in turn limits the overall use of mobile wallets and makes it difficult for consumers to easily use a mobile wallet in person and online. ." We looked at current physical cards and mobile wallets for security vulnerabilities to make our product the most secure. We took microchip technology that consumers trust and used it to create a microchip swipe instead of a magnetic swipe. This makes our product more secure and less susceptible to data breaches. In addition, the card number is not fixed and makes the transaction a transaction. This makes it harder for hackers to steal your data from providers during data breaches, use devices to physically steal your card details, and protect your banking information if our company is ever hacked.

One large issue plaguing the cyber community is the alarmingly high rate of identity theft via stolen or breached data. Some companies may have data leaks and breaches which then lead to information being stolen which is then put up for sale on the darkweb where it can be

purchased. If the information is not put up for sale on the darkweb, sometimes a hacker will use the information directly to commit a crime itself assuming the identity of one of those affected in the data breach by possibly accessing sensitive information that does not belong to the assailant. They can also use the identity they stole to make online and card-not-present purchases.

While many criminals can steal your information via a type of data breach, many others may assimilate that information otherwise by stealing personal property such as a cell phone, smart watch, or computer. Gaining access to such a device with all or most of one's information in one place makes those items easy targets for one who is skilled enough. According to an article sourced from the ODU Library data banks, " System which is the most prone to identity thefts is e-commerce system since the system is growing rapidly. Electronic commerce (e-commerce) is a business paradigm which evolve very fast recently. Most of the retailing and commercial transactions are performed over internet and therefore there is need to establish an information system as the benchmark system. The information system would be enabled for any commercial transaction through the internet. The main users of the information system should be consumers and therefore the system should be user-friendly. Also the system should have a protective module to prevent identity theft." (Vučković et al. 2018) The need for a system to work in the favor of protecting the consumer is necessary, as this article went on to further explain how identity theft plagues the younger generation who more frequently use the internet for purchases and other items. "Due to large prevalence of e-commerce and financial services which leads to availability of big data, there is large significant increasing of identity theft and frauds. There is big online databased which stores sensitive users data with their bank and credit accounts. These databases are prone to hackers' possession. Since there is large increasing of

online banking and shopping sites there transmitting of sensitive personal and financial data over the internet which is prone to attacks. However each used should be aware of the possible risks about the cybercrime. One of the most common cybercrime is identity theft. The identity theft is occurred mostly among students since they use internet more than general population for different purchases and other university tasks. For example many universities have own information systems with personal information about all students which is also prone to identity theft." (Vučković et al. 2018)

We aim to detest such criminal activities with our product by making fraud easier to detect with not only better security, but also the proper more close monitoring of these at risk accounts to ensure that no hackers are tampering with sensitive information. By making transaction data or customer purchase history available, merchants enable issuing bank call center staff to have the information needed to prevent chargebacks, by answering legitimate consumer questions or identifying fraud. Real-time collaboration and data-sharing is one of the most effective tools to reduce fraud.

Another issue we aim to correct with our product is reducing the amount of fraudulent charges that may occur to a consumer. An attack that makes use of a brute force sort of method is called velocity attacks. A velocity attack is when a malicious person repeatedly sends a credit or debit card to make unauthorized payments. They will send the card number until it is verified. They usually get card numbers that have been stolen from a POS terminal. Depending on the software used to launch the velocity attack, it can generate a random sequence of numbers that trigger payouts whenever the sequence is matched with a valid credit card number - usually while the consumer is asleep. As a result, the merchant would start his working day with

unauthorized payments. And as if that wasn't bad enough, this can happen again until the card is full or someone notices these unauthorized transactions. This type of attack is one of brute force and utilizes a Denial of service method or (DDos) which can also serve to disrupt the consumers experience and force them to use other means of completing the transaction, or having to wait or miss out on the opportunity. In this article found via google scholarly articles it states, "In a DDoS attack, the attackers continuously send requests from many authorities to get the web resource down. In e-commerce, for example, they flood the online store, etc., with massive traffic and make the customers unable to purchase something (Anshari et al., 2022). This leads to the disability of the online firm for hours or even for several days. And if the attack is in peak season, it is more annoying and severe; it may cost a considerable amount in the form of customer and income loss (Dahiya and Gupta, 2020). The primary purpose is to make service delivery impossible by thwarting online firm or store access. It can be of many forms and depends upon the purpose of the attackers and the nature of the e-commerce firm or store (Mishra et al., 2022). (Liu et al., 2022) This form of cyber attack is becoming increasingly more prevalent and frequently used by attackers, which allows them to have the upper hand when controlling the situation regarding security for sensitive information.

Our product plans to combat this problem by working to incorporate better authentication to help prevent from fraudulent charges, as well as having multiple security measures that ensure when a system becomes overloaded and therefore compromised, that it shuts down and doesn't allow anyone access with the network and is functions unless in the physical location of the servers. This makes sure that anyone who may be participating in a multi stage attempt to access information behind security is not able to intercept any data from private connections. Within

the verification for our product, we will ensure that not only do we use some form of 2 factor authentication via biometrics to make sure that unauthorized individuals are not afforded access to our consumers data. Biometrics are something that can not be easily fabricated for an attacker to use. This is more appealing as a business because security questions can be answered by attackers with proper information. Via biometrics, the attacker cannot possibly come up with a way to bypass either a face scan or fingerprint, thus giving no access to the assailant rendering them useless.

Attackers can also use a device spoofer to attempt to steal information from a consumer's personal device, or attempt to take over their accounts and use them for nefarious purposes. This kind of fraud is committed through tricking the system into thinking that the requests being sent are coming from one device, but are truly coming from another. This type of attack is almost like a form of camouflage for the attacker due to the difficulty in pinning this type of attack. As mentioned previously in this paper, there are many tools on the open web that if properly used, allow you to conduct such activities anonymously. To those who are more experienced or knowledgeable, they may source help from the dark web where they can purchase either services or tools to carry out the attack for them with a greater amount of anonymity which poses a serious threat to not only our business, but many others as well.

These attacks have a range of different forms and can be as simple as being victim to a type of phishing attempt, which bait the user into clicking on a link that may look legitimate but is in fact not and can be used as either a backdoor, or an open pathway for malicious software such as trojans. These spoofers require the use of some sort of VPN to artificially create an IP from which they can attack from. Our business plans to eradicate the use of those through a

similar method that Sports Betting and Gambling take, which is not allowing the use of accessing information while using a VPN. We are going to make using a VPN alert other companies when an unauthorized IP accesses their information as the IP addresses are not unique to the user only the service. This will be against the account operating rules, meaning that the account will not load until the VPN is turned off or temporarily disabled, eliminating the use of spoofers to try and access information illegally.

Lastly our product intends to keep our partners safe from the use of card skimmers and other such devices that take your information from you without your knowing. These kinds of attacks are carried out in the physical world, though can be done with man in the middle attacks via networks. This differentiates them from the others that were mentioned before it as those were all mainly ones that occur in the cyber domain. Card skimmers can be employed on a number of different devices without the user being aware of the tasks being performed. Many of these devices can be found at everyday places such as gas station pumps and store card readers. Since card skimmers are physical items, they are much easier to see for those who are paying attention. They are detectable and oftentimes have tell tale signs of temperament at the station you plan to use.

Our product plans to try and lower the need for card readers, and instead use contactless methods using NFC (near field communication), to transmit data safely and securely. We plan to employ this through the use of R-FID (radio frequency identification). This detection method is far superior than normal card readers as the card is not able to communicate with the device, meaning that anyone could read that information being transmitted over the radio waves.

According to an article found through ODU's library database, "Detection consists, by using a tag reader, in first finding objects that emit signals with sufficient power to reach the reader, wherever they may be hidden, and second getting some information about them. Thus, provided the level of information given by the tags is appropriate, every accounting application can be fulfilled by this procedure (see above the customs example). However, when the level of information which is publicly available from the tags is too high, privacy concerns arise, as provided data could allow anyone to uniquely (or almost uniquely) identify each tag. Therefore, it becomes necessary to design a general scheme for RFID tags and readers, which allows tags to disclose the nature of the items they are included in, without identifying themselves uniquely to any tag reader." (Mobahat, 2010). This would help resolve the issue of having sensitive information be better protected when being transmitted as to not allow attackers to steal that data when vulnerable. The use of RFID also helps to better authenticate the physical transactions as to better protect the consumer and their data.

During my time at Old Dominion, I have tried to branch out in the courses that I take to broaden my knowledge. One course that brought intrigue to me was a state and local policy course that I took overseeing the process of how state and localities conduct their business, along with the workings of how policy is made and passed and what processes are undergone to achieve that. The integration of electronic transactions into the physical world has been interesting for many years and as the world continues to evolve, so does the way we deal. Electronic transactions have changed the way money is handled, but that doesn't mean it's without its challenges. Electronic transactions, like any other transaction, are vulnerable to fraud

and other forms of cybercrime. To bring electronic transactions into the physical world, making them safer and easier to implement, the state and municipalities must play a decisive role.

One of the most important ways that state and local policies help integrate electronic transactions into the physical world is by investing in the necessary infrastructure. Electronic transactions require a reliable and secure digital infrastructure to operate effectively. This infrastructure includes hardware, software and network resources that must be regularly maintained and updated. The state and municipalities can contribute to the existence of this infrastructure by providing funds and resources to support the development and maintenance of the necessary infrastructure. In this way, companies and individuals can trade safely and reliably.

State and local governments can play a part in tending to the issue of e-transaction fraud. E-transaction fraud is a major concern for both businesses and buyers, and state and local governments have a duty to protect their citizens from false action. This may incorporate passing laws that require financial institutions to implement certain fraud prevention measures, or advertising assets to businesses and buyers to assist them ensure themselves from fraud. The issue of bringing e-transactions to the physical world whereas making them more secure and simpler to conduct is an imperative issue that relates to state and local legislative issues in numerous ways. States have the control to direct money related educate, commerce, and cybersecurity, and they can play a part in advancing the selection of e-transactions and addressing the challenges related with e-transaction extortion. By working together, state and nearby governments can offer assistance to form a more productive and secure monetary framework that benefits businesses and shoppers alike.

One way state and local governments can help in the integration of e-transactions into the physical world, is by advertising motivations to businesses and people who receive e-transactions. The government could offer tax credits or other motivating forces to any businesses willing to use our NFC card for physical and e-transactions as a means of payment. By doing so, they would empower more businesses to embrace our product, which would help to increase the use of e-transactions in the physical world. This would help to create a more secure and helpful payment system, which would benefit both businesses and buyers. State and nearby legislative issues can moreover play a part within the improvement of organizations between the open and private sectors to promote the integration of e-transactions into the physical world. The government can work with private businesses and organizations to create inventive arrangements that empower businesses and people to conduct both physical and e-transactions using our product in a secure and reliable way. Our business will be able to share assets, information, and skill, which would offer assistance to form a more vigorous e-transaction system for better consumer safety and regulation.

As the world becomes more digitized, payment methods have evolved to provide more convenience and ease for consumers. The emergence of e-transactions has revolutionized the payment industry, but it still poses challenges, especially when it comes to bridging the gap between e-transactions and physical transactions. As digital payments continue to gain popularity, the need for secure and effective payment methods is increasingly important. A contactless universal payment method, which allows individuals to make transactions without physical contact, has the potential to be both safe and efficient. However, it also raises concerns about security, including the risk of fraud and data breaches. To address these concerns, a

combination of security measures can be used, including firewall systems, biometric scans, 2-factor authentication, and cryptography.

A firewall is a security framework that screens and controls incoming and outgoing network activity. It acts as a boundary between a private organization and the web, and makes a difference preventing unauthorized access to the organization. Firewall frameworks can be effective in securing a contactless universal payment method by avoiding malevolent actors from accessing the payment system. Firewall frameworks are a vital component of a secure contactless payment framework. They can offer assistance and can help prevent unauthorized access to the payment system and identify and avoid attacks.

Biometric checks are a progressively well known security degree for computerized installments. Biometric verification includes utilizing physical characteristics, such as fingerprints or facial acknowledgment, to confirm a user's character. Biometric checks can be utilized in conjunction with other security measures, such as passwords or PINs, to supply an additional layer of security. Biometric filters can be especially successful in securing contactless payments, as they can be utilized to confirm a user's personality at the point of deal. For illustration, a client may be required to filter their unique finger impression or face to confirm a transaction. This could offer assistance to anticipate false transactions, as it guarantees that only authorized clients are able to create payments.

Two-factor verification (2FA) may be a security process that requires clients to supply two forms of recognizable proof to get access to a system or perform an exchange. The two forms of identification ordinarily incorporate something the client knows, such as a secret word, and something the client has, such as a token or a shrewd card such as a mobile app. The use of

2FA makes a difference to avoid unauthorized access and fraud by requiring an extra layer of confirmation past a secret word or other fundamental security measures. Within the setting of contactless universal payment strategies, 2FA can be utilized to supply an extra layer of security past the contactless payment innovation itself. For example, a client can be required to enter a password or Pin to access their account, and after that also use a token or form of identity to confirm. This would help to anticipate unauthorized access to the account, even on the off chance that an aggressor managed to trigger the contactless payment signal.

Cryptography is the practice of securing communication from third-party interference. Cryptographic methods are utilized to guarantee privacy, astuteness, and genuineness of the information being transmitted. Cryptography is utilized to encode messages so that as it were the planning beneficiary can decode it. Cryptography can too be utilized to distinguish unauthorized changes to information, and to confirm the realness of a message. In the setting of contactless universal payment methods, cryptography can be utilized to secure the transmission of installment data from the point of deal to the installment processor. One illustration of cryptography that's commonly utilized in contactless installments is the utilization of scrambled communication conventions, such as SSL/TLS. These conventions scramble the communication between the installment terminal and the installment processor, guaranteeing that the installment data cannot be intercepted by aggressors.

The invention of a universal payment method that bridges e-transactions and physical transactions is an idea that has been talked about for many years. While the idea itself is sound, the challenge lies in turning it into a reality. In order to do so, there are several key factors that must be considered.

First and foremost, any universal payment method must be secure. When it comes to electronic transactions, security is of the utmost importance. Consumers must feel confident that their personal and financial information is safe when they make purchases online or through mobile devices. Therefore, any universal payment method must incorporate the latest security measures, including encryption and multi-factor authentication.

Secondly, the payment method must be easy to use. Consumers are accustomed to a certain level of convenience when it comes to making payments, whether it's through credit cards, cash or online payments. Therefore, any new payment method must be user-friendly and easy to navigate. It should be accessible to anyone, regardless of their level of technical expertise.

Another important factor to consider is interoperability. A universal payment method must be able to work with a wide range of devices and platforms, including smartphones, tablets, laptops, and point-of-sale systems. This requires a significant amount of collaboration between technology companies, financial institutions, and merchants. In addition, any universal payment method must be scalable. As more and more consumers adopt the new payment method, the infrastructure must be able to handle the increased volume of transactions. This means that the payment method must be able to support millions of users and transactions per day.

Furthermore, another important consideration is regulatory compliance. Any new payment method must comply with local and international regulations, including those related to data privacy, fraud prevention, and consumer protection. Failure to comply with these regulations could result in significant fines and damage to the reputation of the payment method.

In terms of implementation, a universal payment method must be supported by a robust marketing and education campaign. Consumers must be made aware of the benefits of the new payment method, as well as how to use it. This requires a significant investment in marketing and public relations.

Finally, any universal payment method must be financially viable. This means that it must be able to generate revenue for the companies involved, whether through transaction fees, licensing fees or other revenue streams. The financial viability of the payment method is critical to its long-term success. Turning the invention of a universal payment method that bridges e-transactions and physical transactions into a reality requires careful consideration of a wide range of factors. Security, ease of use, interoperability, scalability, regulatory compliance, marketing and financial viability are all critical components of a successful universal payment method. By carefully considering these factors and working collaboratively, it may be possible to turn this idea into a reality that benefits consumers, merchants and financial institutions alike.

The following steps will definitely be to urge the use of this product on the market for shops and businesses alike to utilize. The next step going forward is embracing the outcome naturally. I would like the product to develop in a natural way in which those it touches can see the benefit of streamlining such a service. What I had known beforehand was nothing compared to what I know now being so naive about such a project. During this experience I never expected this to come about, though it is welcome to have such a clash of ideas. Being in a group, this project is a reflection of everyone in our project. As a group I want my card to reflect that and if it doesn't then it does not help me. This card needs viable security, adjustment, and innovation in order to really be effective. I commend the makers of the original mobile wallets

as I know it took time to urge this idea to others in the industry. We as entrepreneurs needed to progress the portable wallet with the e-wallet so we had a part on the table too. Things that I would have done in an unexpected way is have more individual discussion with my bunch, at that point I would have felt the gather involvement more. We had different zoom calls but I feel as in the event that we might have tired individuals more. We seem to have had thoughts that went smoother and were more progressed. Our current product is reliable and seems to outperform the portable wallets offered currently on the market. Our products innovation and creativity as well as the well being of safety and security that went into the idea shows me the collaborative work we conducted over the semester as almost a fruit of my labor.

References

Kahn, R. (2021, October 13). What Is Device Spoofing? How Is It Different from Domain Spoofing? Retrieved April 21, 2023, from https://www.anura.io/blog/what-is-device-spoofing#:~:text=Spoofing%20is%20a%20practice%20where,marketing%20partner%2C%20or%20website%20owner.

Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2018). ATM card cloning and ethical considerations. *Science and Engineering Ethics*, *25*(5), 1311–1320. https://doi.org/10.1007/s11948-018-0049-x

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.927398

Mobahat, H. (2010). Authentication and lightweight cryptography in low cost RFID. *2010 2nd International Conference on Software Technology and Engineering*. https://doi.org/10.1109/icste.2010.5608776

Saleh, Z., PhD. (2013). The Impact of Identity Theft on Perceived Security and Trusting E-Commerce. Journal of Internet Banking and Commerce, 18(2), 1-11. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/impact-identity-theft-on-perceived-security/docview/1449792093/se-2

Suryadi, A. (2021). Responsiveness of criminal law to skimming crimes in the era of Industrial Revolution 4.0 (Four point zero). *Jurnal Hukum Volkgeist*, *5*(2), 130–142. https://doi.org/10.35326/volkgeist.v5i2.845

Vučković, Z., Vukmirović, D., Milenković, M. J., Ristić, S., & Prljić, K. (2018). Analyzing of e-commerce user behavior to detect identity theft. *Physica A: Statistical Mechanics and Its Applications*, *511*, 331–335. https://doi.org/10.1016/j.physa.2018.07.059

Yang, J., Chen, Y., Trappe, W., & Cheng, J. (2014). Detecting Mobile Agents Using Identity Fraud. In *Pervasive Wireless Environments: Detecting and localizing user spoofing*. essay, Springer International Publishing.