# ASSESSING MOBILE PAYMENT SECURITY THROUGH SSL PROXYING: AN ANALYSIS OF POPULAR PAYMENT METHODS

Jordan McCready, University of North Georgia

Tamirat Abegaz, University of North Georgia

Jason Porter, University of North Georgia

Cindi Smatt, University of North Georgia

## ABSTRACT

Mobile payments have become increasingly popular due to their convenience, speed, and ease of use. There are various mobile payment options available, including Apple Pay, Google Pay, Venmo, PayPal, and Cash App. However, with mobile payments being relatively new, it's essential to understand the potential security risks associated with these options, such as the potential for mobile payment companies to gather a customer's personal information for fraudulent activities. This project aimed to explore these risks and compare the features and functionalities of five popular mobile payment options: Apple Pay, Google Pay, Venmo, PayPal, and Cash App. The project also focused on determining whether SSL Proxying, a technique used by hackers to intercept and read encrypted data sent over SSL connections, was detected by the mobile payment options studied. Overall, while mobile payments offer a quick and easy way to conduct transactions, users should take appropriate measures to protect their personal information and remain vigilant against potential security threats, should take appropriate measures to protect their personal information, and remain vigilant against potential security threats.

*Keywords*: Mobile Transactions, SSL Proxying, Security, Mobile Payment Apps

## INTRODUCTION

Currency has been a focal point of nearly all civilizations to date. The way we purchase and acquire items has shifted throughout history and will continue to change with time; one current method that is dominating the modern market is mobile payments. In the past, the predominant method of payment was credit cards. However, credit cards have been surpassed by mobile payments as mobile payments allow users to have all their information in one place. The convenience factor in mobile payments is higher as opposed to credit card payments. For instance, Xue and Lin, 2019 found a significant increase in consumers' willingness to use mobile payments over credit cards. Additionally, large financial institutions have witnessed an increase in mobile payment technology over cash purchases (Agarwal, Qian, Ren, Tsai, & Yeung, 2020). Mobile payments can be defined as "a transfer of funds in return for goods and services in which a mobile device is functionally involved in executing and confirming payment" (Taylor, 2016). Mobile payments have begun to revolutionize how people conduct their transactions globally. In 2017, mobile payments made up 3% of the market share of point-of-sale payment methods in the United States, and this percentage increased to 11% by 2021 (*US: Payment methods in retail,* 2021). During the COVID-19

pandemic, many utilized mobile payments for the first time to conduct safe contactless transactions. After the start of the pandemic, over 80 million adults in India and over 100 million adults in China made their first digital merchant payment (*COVID-19 Drives Global Surge in use of Digital Payments,* 2022).

The first mobile payment system was created in 1997 in Helsinki, Finland, where consumers could purchase a Coca Cola beverage from a vending machine simply through an SMS message (Mansuri, 2022). After the creation of SMS-based payments, mobile payments evolved and expanded their capabilities and functions. In 1998, one of the largest and most used mobile payment systems to date was founded: PayPal. The early 2000s brought new ways of utilizing mobile payments, such as purchasing movie tickets on a mobile phone and ordering pizza, and the advancements of cell phones during the early 2000s was a major contributing factor to the continuing growth of mobile payment systems. The high usage of mobile phones has caused many industries such as banking and entertainment to focus their efforts on mobile phone adaptability (Ahmed et al. 2021). In 2011, Google created a digital mobile wallet, and this was the beginning of major corporations adventuring into the world of mobile payments and eventually creating their own systems (Mansuri, 2022). An example of a corporation that has capitalized on the mobile payment market is Apple; this company has branched into mobile payments through the creation of Apple Wallet, Apple Cash, and Apple Pay. The adoption of mobile payments in recent years has begun to increase exponentially. According to Merchant Savvy, "China is the leader when it comes to mobile payments, with 87.3% of the population reported to use contactless payment methods" (*50+ Global Mobile Payment Stats, Data & Trends,* 2022).

There are concerns about the security and vulnerability of all payment systems. According to Bankrate, in 2021, there were nearly 390,000 reports of credit card fraud to the Federal Trade Commission (FTC) with losses amounting to over $6 billion (Bankrate.com, 2023). In recent news, PayPal identified 4.5 million accounts that are believed to have been created illicitly (Kauflin, 2022). Many would raise the question as to how these accounts were created and for what purpose. In 2021, PayPal attempted to bring in new customers by offering five or ten dollars to be deposited into a new user's account if the said person signed up for PayPal or Venmo. This caused problems when bots and/or software were utilized to automatically sign up for PayPal or Venmo, essentially stealing an approximated 22.5 million to upwards of 45 million dollars. One of the main purposes of this project is to compare five of the major mobile payment systems available: Apple Pay, Google Pay, Venmo, Cash App, and PayPal. In other words, this project will outline these five major mobile payments, what their functions include, the security systems in place, how their transactions take place, recent breaches, etc. Two example scenarios of how mobile payments can be abused with little effort will also be highlighted.

## COMPARISON OF MOBILE PAYMENT METHODS

### Apple Pay

Apple Pay was created in 2014 and is compatible with iPhone 6 and newer models. Since 2014, Apple Pay has slowly migrated its way into 74 countries globally, the newest country being Malaysia as of August 9, 2022. Apple Pay is already preinstalled onto every iPhone and is accepted at more than 85 percent of U.S. retailers (*Apple Pay*, 2022). When conducting a transaction on

Apple Pay, the user must submit a two-factor authentication test such as Touch ID, PIN, or Face ID to complete the transaction. Apple Pay also includes a feature called Apple Cash. This feature allows the user to request and/or send money to a recipient through text messaging. Apple Pay can also be used to ride public transportation in countries such as China, the United Kingdom, and the United States (*Where you can ride transit using Apple Pay*, 2022*).* Apple Pay has approximately 507 million users worldwide (*Apple Pay – statistics and facts*, 2022), and it is statistically the most popular mobile payment method in the United States with an estimated 31.2 million more users than Google Pay (Curry, 2022).

On the security side of Apple Pay, it utilizes a few hardware and software to prevent the user's information from being compromised. One component of Apple Pay's security is the Secure Element chip. This chip complies with financial industry requirements for mobile payments because it runs the Java Card Platform (*Apple Pay component security,* 2022). Another component of Apple Pay's security is the NFC Controller. The NFC Controller "handles Near Field Communication protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal" (*Apple Pay component security,* 2022). Essentially, NFC is responsible for keeping the transaction secure. NFC utilizes a maximum range of only a few centimeters to ensure the transaction is not intercepted by possible observers. The third component of Apple Pay's security is Apple Wallet. Apple Wallet is a preinstalled application on iPhones that allows the user to make payments as well as manage credit, debit, and store cards (*Apple Pay component security,* 2022). The fourth component in Apple Pay's security is Secure Enclave. The Secure Enclave is a system on Apple devices that oversees the authentication process and allows a payment to proceed (*Apple Pay component security,* 2022). The last component of Apple Pay's security is the Apple Pay Servers. These servers "manage the setup and provisioning of credit, debit, transit, student ID, and access cards in Apple Wallet" (*Apple Pay component security,* 2022). These servers also manage the Device Account Number that is stored in the Secure Element component. The servers additionally communicate with the payment network or the card issuer servers and the device itself. The last responsibility of Apple Pay's servers is to "re-encrypt payment credentials for payments within apps or on the web" (*Apple Pay component security,* 2022).

**Google Pay**

Google Pay was created in 2011 and can be utilized on iPhones, Android devices, as well as Chrome Operating System Computers. Google Pay is currently available to conduct mobile payments in 54 countries globally (*Find supported payment methods—Google Wallet Help*, 2022). Google Pay does not come preinstalled on Android or iPhone devices and must be installed through their respective application stores. As of March 2022, Google Pay is accepted in an estimated 41% of restaurants, stores, and other point-of-sales in the United States (*Google Pay use per country,* 2022). One of Google Pay's functions is the ability to pay or request money from a group of people through a group chat on the application. Google Pay also keeps track of who has paid their portion and who has not paid. Another function of Google Pay is the ability to track and categorize the user's purchases based on where the purchase was made, even if the purchase was not made with Google Pay. The way Google Pay does this is through the optional functionality of adding your credit card, debit card, transit passes, and business loyalty cards to your Google Pay application. When these extra cards are added to the user's Google Pay app, Google Pay will be able to find

past transactions of all the cards added to the application and where they took place. Google Pay can also show how much the user has spent in the last day, week, or month between the cards that are added to the application. This can be seen as a security risk to some due to potentially all a user's purchases being found in one application but can also be seen as convenient to others. Google Pay also offers Cashback rewards at certain times. According to the Google Play Store, Google Pay has accumulated roughly 500 million Android users since its release (*Google Pay: Save and Pay - Apps on Google Play,* 2022). When a transaction takes place in the Google Pay application, there is a two-factor authentication test before the transaction can be completed. This two-factor authentication test can be completed with a fingerprint scan, lock pattern check, PIN, face ID, or password.

On the security side of Google Pay, one of the security systems in place is a fraud detection system that alerts the user to any fraudulent purchases or risks associated with their account. Google Pay will also tell the user when they are sending or receiving currency from an unknown user or someone who is not on the user's contact list. Google Pay also makes the promise that "Google Pay will never sell your personal information to third parties or share your transaction history with any other Google service for targeting ads" (*Google Pay—Learn What the Google Pay App Is & How To Use It,* 2022). However, Google Pay has the option to "personalize" your experience on the application by utilizing your past and current transactional history. In this sense, "personalize" would be defined as allowing Google Pay to share your transactional history with companies that are relevant to your transactional history. The option to "personalize" the experience of the application is turned off by default. Google Pay also creates a VAN (Virtual Account Number) for the user so no seller has access to the user's real card number (*Google Pay Safety & Security Features—Google Safety Center*, 2022). If the user's mobile device is lost or stolen, the user can remotely lock their Google Account from the Google Find My Device application. Google Pay also utilizes the same technology as Apple Pay to conduct in-person mobile payments, NFC. One of Google Pay's more controversial decisions is the option to not offer buyer protection. In other words, if there are any problems with a purchase through Google Pay, they will not investigate or refund the user's money (*Google Pay—Learn What the Google Pay App Is & How To Use It,* 2022). In recent times, there have been no data breaches or intrusions for Google Pay, but it is only a matter of time before a security breach happens.

**Cash App**

Cash App was created in 2013 and is the number one app under the Finance section of the Apple App Store (*Cash App,* 2022). Cash App is only available in the United States and the United Kingdom. Cash App allows users to send and receive money with an email, phone number, or Cash App's "$Cashtag". Cash App's $Cashtag is essentially a user's profile name on the application. Cash App also offers to send and receive money through QR codes specifically tailored to each user account. Cash App allows the user to purchase, receive and send stocks and Bitcoin to other users; it also gives the option to round up purchases to the nearest dollar and invest the change into stocks of Bitcoin. Like Google Pay, Cash App offers users rewards and discounts on stores and restaurants, such as Bed Bath and Beyond (*Cash App—Save on everyday spending,* 2022). Cash App also has its own card, the Cash Card, which serves the same purpose as Cash App but in a physical card form. The Cash Card also offers even more exclusive discounts to the user. Cash App is available for ages thirteen plus and can file your taxes for no extra charge (*Cash*

*App—Save on everyday spending,* 2022). Cash App has the optional method of paying directly to a mobile payment point-of-sale through the user's mobile device, called Cash App Pay. In quarter four of 2021, it was reported that Cash App had 44 million monthly active users and 13 million users signed up for Cash App Card (Curry, 2022). In 2018, Cash App's annual revenue was 400 million dollars. In 2021, the annual revenue was 12.3 billion dollars (Curry, 2022).

On the security side of Cash App, Cash App offers two-factor authentication, like Apple Pay and Google Pay. When logging into a Cash App account, the user must first enter the phone number registered to the account. Once the phone number is entered, the user's phone will receive a code that has to be entered into the Cash App application. Once the phone number is verified, Cash App will ask for the email address associated with your profile. An email will be sent to the user's email address and will contain another code to enter into the application. Once this code is entered into the application, the user will be logged in. After the user is logged in, they will receive a text message specifying the user's account was logged into. The information in the user's text is the date, time, and location of where the account was logged in from. When a user is attempting to conduct a transaction on Cash App, the user must submit another authorization test in the form of a PIN, Touch ID, or Face ID. The Cash App Card utilizes nearly identical NFC technology as Google and Apple Pay.

Cash App also utilizes the fraud detection system that monitors square point-of-sale terminals, such as a SquareUp Reader. On April 4, 2022, Cash App detected a data breach that affected an estimated 8.2 million users. The actual breach took place in December 2021. This breach stole users' names, bank account numbers, and more (Drapkin, 2022). When considering mobile payments, security is of utmost importance, and therefore security standards have been developed to keep organizations accountable; one such security standard is the Payment Card Industry Data Security Standards (PCI DSS) (Ahmed et al. 2021). Cash App is PCI DSS Level 1 complaint. Level 1 PCI DSS is defined as "a set of security requirements established by the PCI SSC to ensure that all companies that process, store, or transmit credit card or cardholder data maintain a secure environment" (Baykara, 2022). To obtain Level 1 PCI DSS compliance, internal and external security screenings are conducted by authorized independent audit institutions. Cash App manages its internal systems and operations according to a relatively comprehensive list of criteria and rules. In addition, all processes and procedures are subject to detailed on-site audits every year (Baykara, 2022). Cash App also comes with a feature to disable the user's card and account whenever needed. In the case that a Cash App user has a Cash App Card, the user will have their money insured up to 250,000 dollars if the user's bank goes out of business by the FDIC (Federal Deposit Insurance Corporation). The FDIC, however, does not cover the user's money that is lost to fraud on the Cash App application. Like PayPal, Cash App often offers five or ten dollars to people who create a Cash App account and invite their friends. This could prove to backfire for Cash App like it has for PayPal, but it has yet to be documented.

**PayPal**

PayPal was created in 1998 and conducted over 19 billion transactions in 2021 (Curry, 2022). PayPal, like Google Pay, Apple Pay, and Cash App, supplies users offers and cashback on certain companies. PayPal's central focus is the ability to send and receive currency in almost every region on Earth. The application can be accessed on IOS devices, Android devices, and computers.

PayPal, like the other mobile payments, has a rewards program that rewards the user points whenever the user conducts a transaction. These points can be redeemed for direct transactions through PayPal or can be redeemed for charitable donations (*PayPal Rewards Program,* 2022). One function of PayPal that the other mobile payments discussed do not have is the ability to pay for purchases over time and customize when and how much is paid overtime. PayPal also offers a physical card known as the PayPal Cashback Mastercard. This card offers the users unlimited 3% cashback on PayPal purchases and unlimited 2% cashback on other eligible purchases (*PayPal Rewards Program,* 2022). PayPal users, like Cash App, can purchase and sell Bitcoin. PayPal expands on Cash App's cryptocurrency stocks by adding Bitcoin Cash, Ethereum, and Litecoin to be purchased and sold by their users. The application can also deposit checks and scan QR codes as a form of payment. Another function of PayPal is to manage the user's bills from the application itself. In 2021, PayPal made an estimated 25.3 billion in revenue, and has reported an increase in annual revenue each year since 2010 (Curry, 2022).

Recently, PayPal acknowledged that 4.5 million accounts were created fraudulently to take advantage of the new user sign-up promotion. In 2020, a hacker named Alex Birsan discovered a security vulnerability in PayPal and reported it to PayPal's Bug Bounty Program. While exploring PayPal's authentication flow, he discovered a JavaScript file with a session ID that could potentially allow attackers to exploit the data. Birsan then tested an XSSI vulnerability on the JavaScript file and found that the session ID was still visible in plain text, but this alone was not enough to impersonate a user's account.

After examining PayPal's main login form, Birsan discovered that after a few failed login attempts, users would be required to solve a reCAPTCHA challenge before trying again. A reCAPTCHA challenge involves choosing which photos are appropriate for a given question. If the challenge is solved, an HTTP POST request is initiated, which allows data to be sent to the server. Birsan found that he could obtain a victim's PayPal email address and password if he performed an HTTP POST request test with the right timing and user-interaction, while knowing all the tokens used in the request. Birsan reported his findings to PayPal's Bug Bounty Program, and he was awarded $15,300 for his discovery on December 10, 2019. PayPal fixed the vulnerability within five days after the award was granted. (Birsan, 2020).

One of PayPal's security systems in place is the PayPal Security Key. This Security Key is a free layer of security at login, like two-factor authentication previously mentioned. The user upon login will be prompted to enter their password as well as an OTP (One-Time PIN) that is unique per login attempt. PayPal also has in place a fraud detection system, like the other mobile payment options mentioned, where the user can be texted, called, or emailed alerts when any attempt at a fraudulent login or charge has taken place. PayPal's security also utilizes Key Pinning to establish TLS (Transport Layer Security) connections from the user's mobile device into a verified PayPal server, preventing fraudulent interceptions from occurring. Key Pinning can be defined as "an Internet security mechanism which allows HTTPS websites to resist impersonation by attackers using mis-issued or otherwise fraudulent digital certificates" (*Public Key Pinning/Certificate pinning,* 2022). PayPal, like Cash App, is PCI DSS Level 1 complaint. PayPal has partnered with the company HackerOne to encourage the findings of vulnerabilities in PayPal's systems by ethical hackers and to report these findings through PayPal's Bug Bounty Program.

**Venmo**

Venmo was created in 2009 and is only available in the United States. In 2014, PayPal purchased the parent company to Venmo, Braintree, for 800 million dollars (Krosofsky, 2020). In 2021, Venmo made an estimated 850 million dollars, a 44% increase from 2020 (Curry, 2022). Like Cash App and PayPal, Venmo offers their users a physical card to be able to earn up to 3% cashback when the user sends or spends on the Venmo account (*Venmo—Share Payments,* 2022). The Venmo Credit Card also displays a personal QR code on its front to make transactions faster. The Venmo Credit Card displays all card activity for the user to manage in one spot, like Google Pay. The Venmo Credit Card also allows users to share and split purchases with other users (*Venmo—Share Payments,* 2022). Venmo offers users another optional physical card, the Venmo Debit Card. This debit card also allows the user to track, split and share purchases through the application. The debit card also can be withdrawn from an ATM if needed. Venmo cards provide contactless shopping for Venmo's users. Venmo, like Cash App and PayPal, allows users to invest in cryptocurrencies including Bitcoin, Ethereum, Bitcoin Cash, and Litecoin (*Crypto on Venmo*, 2022). The users can also toggle price change alerts on cryptocurrencies and decide how much the user wants to invest daily. The application's users must be age 18 plus to utilize Venmo. Venmo can be accessed by Apple devices, Android devices, and computers. In 2021, Venmo reported 70 million users (Curry, 2022). Another function of Venmo is the ability to use the user's funds to purchase items at their featured partners, such as Door Dash and Foot Locker. When a user is attempting to login into Venmo, like the other mobile payments, the user will have to complete a two-factor authentication test. This test will send the user a text message with a code, and then the user will place this code into the text box provided on the application to log in.

On the security side of Venmo, Venmo offers security researchers the chance to report vulnerability findings to the same program PayPal utilizes, the PayPal Bug Bounty Program. Venmo also offers the user an additional means of security in the form of Face ID and/or a PIN. One interesting possible security issue with Venmo is the Venmo Credit and Debit Cards. These cards present possible issues due to the company's data collection. The data collected from these cards are utilized to offer recommendations in the form of Venmo's reward system. However, although this may seem convenient for the user, it also proves that Venmo is reviewing the transactional history from the user's card to "personalize" their experience, like Google Pay. One difference between Venmo and Google Pay in this instance is that Google Pay offers the users the ability to turn off the "personalize" option, while Venmo does not. Venmo is PCI DSS complaint.

Dan Salmon, an Information Security graduate, discovered a security vulnerability in the mobile payment app Venmo in 2019. By analyzing his phone's network traffic, he found that a public API endpoint was returning data to the feed, allowing anyone to request the latest twenty transactions from around the world without authorization (Salmon, 2019). Salmon wrote a 20-line Python script to scrape the API endpoint and found that he could download an estimated 115,000 transactions a day, potentially exposing sensitive information about Venmo users, including which other applications they were using, and transactions made for illegal goods. Salmon concluded that unethical hackers could use this vulnerability to launch spear phishing attacks on Venmo users and recommended that users change their privacy settings to prevent this vulnerability from being exploited (What is Spear Phishing? Definition, Risks and More, 2022).

An API is an interface that allows companies to open their applications' data and functionality to external third-party developers and business partners, and Salmon found that Venmo's API endpoint could be accessed outside of the application without authorization (IBM, 2020). This vulnerability highlights the importance of implementing proper security measures to protect user data in mobile payment applications. Salmon's findings demonstrate that even with a limit of two transactions per minute per IP address, unethical hackers could potentially access large amounts of sensitive information and use it for malicious purposes. Venmo users should be aware of the risks associated with using the application and take necessary steps to protect their privacy and security (HTTP Methods GET vs POST, 2022).

| | **Apple Pay** | **Google Pay** | **Cash App** | **PayPal** | **Venmo** |
|---|---|---|---|---|---|
| **Year Created** | 2014 | 2011 | 2013 | 1998 | 2009 |
| **Users (2021)** | 507 million | 500 million | 44 million | 426 million | 70 million |
| **Availability** | 74 countries | 54 countries | UK & US | Most regions | US only |

Table 1: Summary of comparison of five mobile payment option

## METHODOLOGY

In this section we discuss the methodology used to analyze the security of five major mobile payment applications.

### Data Collection

Square is a company that provides mobile payment solutions, and it has grown in popularity due to offering relatively cheap options for small/local business to receive mobile payments. A SquareUp Reader for Chip and Card has the capacity to take mobile payments through Apple Pay, Google Pay, and Cash App. A SquareUp Reader was purchased to analyze these three methods of mobile payments, and it was used in connection to an iPhone 7. A Square account was created, and the associated “business” attached to it was named “Collectibles.” This fake business account was used to collect data for this project. Two accounts from each mobile payment service (Apple Pay, Google Pay, and Cash App) were collected, creating a sample size of six. The mobile finical transaction was performed by a member of the researchers. Two of the target mobile payments, Venmo and PayPal, are not accepted by the SquareUp Reader. Therefore, these applications were downloaded to an iPhone 7 and transactions were made directly through the app. Two accounts for PayPal and two accounts for Venmo were collected and analyzed.

### Mobile Payment Experimental Scenarios

The first experimental scenario that was explored with mobile payments used the Square fake business “Collectibles.” With Collectibles, the owner of the Square Account can add customers to a database when conducting a transaction. Many companies have similar systems in place that ask customers for their phone number, name, address, or email in exchange to sign up for coupons or a rewards program. This first experimental scenario aims to answer the question, could the hypothetical owner of Collectibles utilize this system for personal gain? The first scenario is quite a real possibility in today’s world. To begin this scenario, the owner of Collectibles could ask a

customer if they would like to sign up for the "Rewards Program." If the customer says no, the scenario is halted. However, with enough volume of customers, the owner is bound to get at least one customer to sign up. If a customer agrees to join the rewards program, the owner could potentially ask for their name, address, email, and phone number, but it is not likely that a customer would give all this information away. For this scenario, the owner will only ask for their name and phone number. Once this information is recorded and stored into the customer database, the owner could now potentially utilize this information to figure out more details about their customers.

The second experimental scenario that was explored with mobile payments was also observed through the perspective of the owner of Collectibles. When a transaction is conducted on the SquareUp Reader, the owner has the option to email or text the customer their receipt. When the transaction is complete, the owner can review the receipt in the Square Application. This receipt includes the last four digits of the customer's card. This experimental scenario raises the question, could the hypothetical owner of Collectibles attempt to figure out the rest of the customer's card number? The second scenario is more hypothetical than the first scenario. In this second scenario, the owner would observe the receipts from previous customer transactions. These receipts would show the owner the last four digits of the customer's card and what card type the customer paid with. To simulate how the owner could predict if a card number is valid from only having the last four digits and guessing the rest, the Luhn's Algorithm was used. This algorithm is defined as "a formula used to validate a variety of identification numbers, such as credit card numbers" (*Luhn algorithm,* 2022).

**Data Analysis Tool**

The forensic tool utilized for this project was Charles Web Debugging Proxy. This program can directly observe network traffic and determine what programs or software were utilized on a mobile device or computer in each time slot. Charles can also act as a "man in the middle" for SSL Proxying attacks. For the utilization of this project, the SSL Proxying feature of Charles was the only feature that was tested. SSL Proxying is defined as a "transparent proxy that performs Secure Sockets Layer encryption (SSL) and decryption between the client and the server. Neither the server nor the client can detect its presence" (*What is a SSL Proxy? Definition & Related FAQs,* 2022). Essentially this means that Charles can observe oncoming network traffic packets and decrypt what is located inside these packets if SSL Proxying is enabled. In theory, neither the server of the application nor the client of the application should be able to detect the SSL Proxying. This project tested if the five mobile payment options would detect the presence of the SSL Proxying attack and what reaction the applications would have if the SSL Proxying is detected.

To enable SSL Proxying on Charles and the iPhone 7, there were a few steps to complete before this could happen. The first step was to install Charles Web Debugging Proxy onto a computer. The second step was to set up Charles to observe the iPhone 7's network traffic. To accomplish this step, the research group had to go to iPhone 7's settings and from there Wi-Fi settings were selected. From Wi-Fi settings the Configure Proxy was selected. On Configure Proxy, since Charles stated that 8888 was the port number for connecting mobile devices to Charles, 8888 was used as the port number and the default IP was selected. Once the Proxy was configured on the iPhone 7, Charles automatically detected the iPhone 7 and allowed the researchers to record the network traffic coming from the iPhone. At this point, Charles could record network traffic, but it

could not decrypt what was sent in the requests from the applications. This is not a function utilized for this experiment, however, to enable SSL Proxying the researchers had to solve this problem. To solve this, the Safari Application on the iPhone 7 was accessed to download the certificate of SSL Proxying by Charles onto the iPhone 7. A certificate in this sense is "a unique, digitally signed document which authoritatively identifies the identity of an individual or organization" (*What is a Certificate?* 2021). This specific generated certificate can be utilized on websites and/or applications in place of the authentic certificate a website and/or application is supposed to have. Once this certificate was downloaded, it was able to determine which mobile payments were detecting the SSL Proxying and which ones showed no signs of detection through Charles.

## RESULTS

### Mobile Payment Experimental Scenarios

The first experimental scenario's goals were to find as much information as possible from only the name and phone number of the hypothetical customers: Dante and Sadie. With just the phone number of Dante, member of the research group was able to discover a few pieces of personal information from "usphonebook.com." The first thing member of the research group found was Dante's real name. From there, within seconds a member of the research group was able to locate Dante's address, phone type, the carrier of the phone, and relatives. member of the research group was also able to find Dante's former address, former phone number, and age very easily as shown in Figures 1 and 2 below.

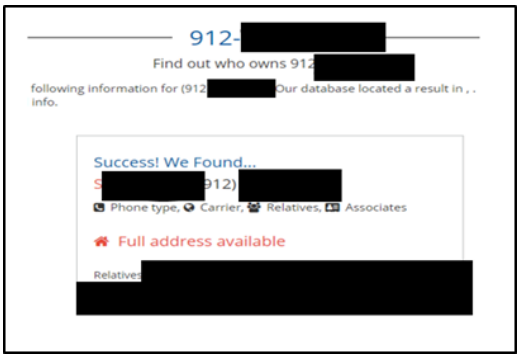


Figure 1: Information gathered on "usphonebook.com" from Dante's phone number and name.

From this discovered information, all of Dante's relatives' numbers, addresses, ages, and prior addresses and phone numbers could be found with further searching. In many cases most database websites, like White Pages, will make the user pay for this personal information. However, we utilized usphonebook.com so the information was free and relatively easy to find, which can be frightening when considering the security concerns.


Figure 2: Additional information gathered on "usphonebook.com" knowing Dante's phone number and name

Using Sadie's phone number, member of the research group was able to find their name, age, address, relatives, former addresses, and phone numbers from "usphonebook.com." To gather more information, member of the research group utilized another website called "Spokeo.com." On Spokeo, member of the research group was able to search Sadie's actual name and gather additional information including a Google Maps representation of Sadie's former addresses, the number of bathrooms and beds in their present address, how long Sadie has lived there, and three former phone numbers with the activation location and service provider attached to the phone numbers as shown in Figure 3. If someone had wanted to dive further into Sadie's relatives and figure out their personal information, this could have been done with relative ease. With Spokeo, a member of the research group did not have to purchase any of the information, and it was found within seconds of searching Sadie's actual name.


Figure 3: Information gathered on "Spokeo.com" knowing phone number and name.

In the second experimental scenario, member of the research group mentioned the fake example card numbers of "4556 7375 8689 9855" and "4024 0071 0902 2143." These card numbers were tested to see if they were valid or not through the Luhn's Algorithm. The member of the research group utilized the first card number, "4556 7375 8689 9855" for the first part of this scenario. The first step of Luhn's Algorithm was to start at the second to last number on the right, in this case 5, and from this point skip every other number moving from right to left. The numbers not skipped, 5,9,8,8,7,7,5, 4, were doubled. When these numbers were doubled, however, numbers that were more than one digit were added up after being doubled. In this example, the 5 was doubled to 10

but to comply with Luhn's Algorithm, the 10 turned into 1+0 which added to 1. The resulting numbers left to right were 8,1,5,5,7,7,9,1. The next step was to add these numbers up to get 43. The numbers that were skipped, 5,8,9,6,5,3,6,5, were added to the previously established 43. These numbers added to the 43 was a total of 90. If the last digit ends in a 0, the card number is valid. In this case the card number could be validated through the Luhn's Algorithm. The second card number, "4024 0071 0902 2143", was utilized next. member of the research group followed the same steps as before. member of the research group started at the 4 in "2143" and skipped every other number, and following the same process as mentioned above this resulted in the final set of 8,4,0,0,5,0,0,4,8. These numbers were then added up to equal 29. The numbers skipped, 0,4,0,1,9,2,1,3, were then added up to equal 20. When adding 20 and 29, we got 49 which proved that the card number is not valid.

**Apple Pay Results**

The first mobile payment option that member of the research group attempted the SSL Proxying on is Apple Pay, furthermore the Apple Wallet application. The first transaction on Apple Pay was through the SquareUp Reader. member of the research group enabled SSL Proxying and had Charles record the network traffic as shown in Figure 4. The highlighted line in Figure 4 represents that the certificate member of the research group had downloaded onto the iPhone 7 for SSL Proxying had been accepted. Before and after the transaction occurred, the research group had no errors, or any security measures detecting the SSL Proxying. The second transaction on Apple Pay has similar results. The only difference in the transaction network traffic was the highlighted line in Figure 5, which displays a notification that was sent to the customer's Visa card to indicate that the purchase was successful even with the SSL Proxying on.

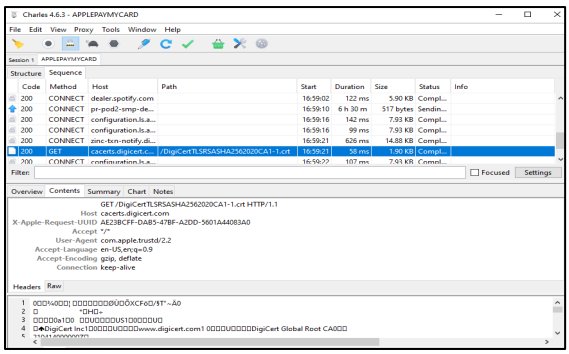


Figure 4: First Apple Pay transaction network traffic.

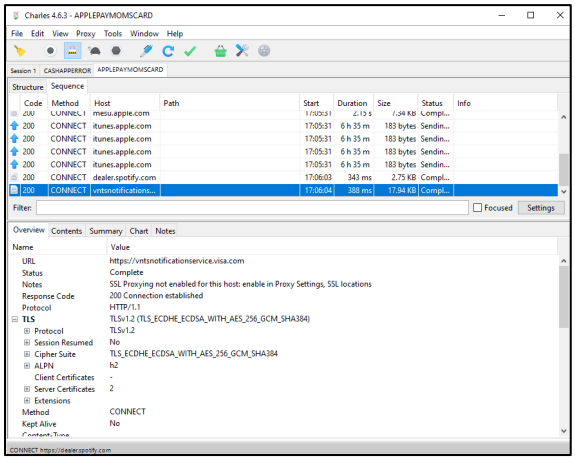

Figure 5: Second Apple Pay transaction network traffic.

## Cash App Results

The second mobile payment option that members of the research group attempted this test on was Cash App. Cash App's results were not what members of the research group expected initially. When SSL Proxying was enabled, Charles and Cash App had responses different from Apple Pay. In Charles, it was observed that Cash App had initially accepted the certificate as shown in Figure 6. After Cash App initially accepted the certificate, the research group was planning on conducting the transaction but noticed the following message on an iPhone 7 (shown in Figure 7). After receiving this message, the notification was accepted. The research group also observed the error on Charles and was left with the following message shown in Figure 8. This message indirectly told Charles that SSL Proxying was detected and because it was detected, no further communication was established with Cash App. The second attempt of a Cash App transaction resulted in the same error message on the iPhone 7 and a different error message on Charles as shown in Figure 9.

A socket write error can be defined as a Windows operating system error that is due to a failure to secure the client's network layer to the receiving server. From this error it was concluded that the SSL Proxying was detected again by Cash App through the socket write error.

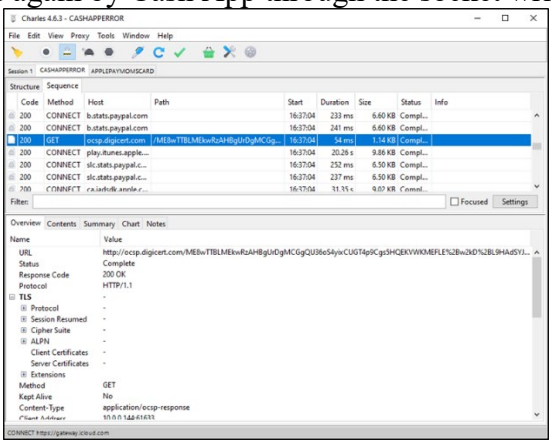

Figure 6: First Cash App transaction initial certificate.

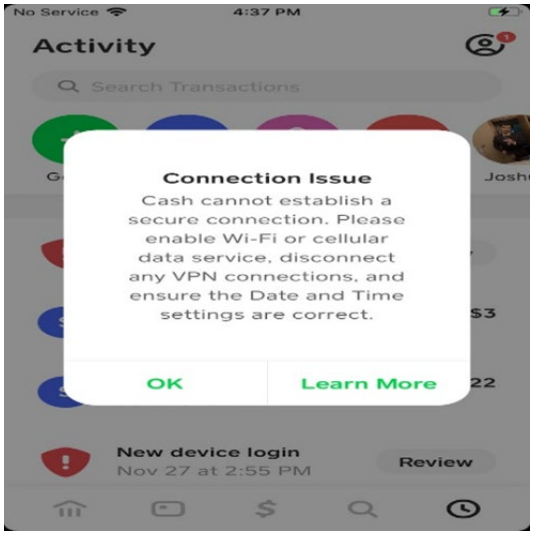


Figure 7: Error message when attempting to conduct Cash App transaction.

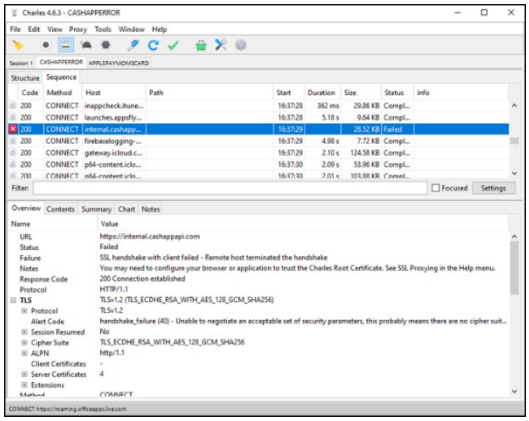

Figure 8: Cash App error message on Charles after first attempted transaction.

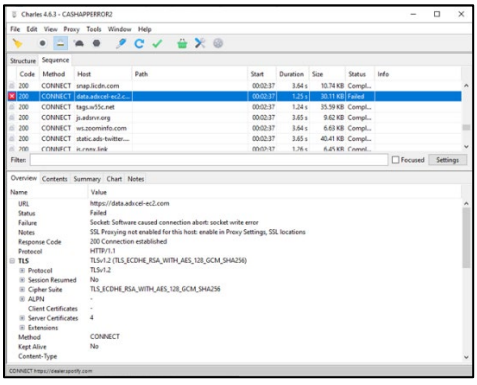

Figure 9: Cash App error message on Charles after second attempted transaction.

## Venmo Results

The third mobile payment that the researchers used utilized for this test was Venmo. The first transaction on Venmo was a success. The transaction proceeded without any detection method or any error on the iPhone 7 application. While observing the network traffic it was noticed that the

Venmo ID number and name were in plain text after SSL Proxying as shown in Figure 10. When observing the network traffic from Venmo, the research group noticed that the certificate was checked twice and verified by Venmo as shown in Figure 11.

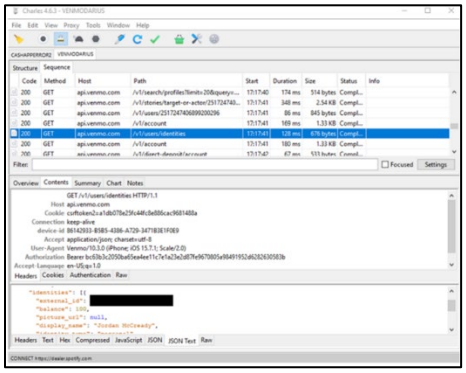

Figure 10: First Venmo transaction displaying personal Venmo ID and name

**Google Pay Results**

The first transaction of Google Pay was successful. On the Google Pay application, there were no errors or any signs of the SSL Proxying being detected. Figure 12 shows where Google Pay checked and verified the validity of the certificate. The second transaction on Google Pay was also a successful transaction. When observing the network traffic on Charles, the researchers noticed that there was a network packet that displayed the access token and the token ID of the transaction as displayed in Figure 13.

**PayPal Results**

The first attempt at a transaction on PayPal while SSL Proxying resulted in the following message on the iPhone 7 as shown in Figure 14. This message did not show up for a minute and thirty seconds after the research group opened the application on the iPhone 7. However, on Charles, the certificate was not visibly trusted or mentioned on the network traffic. One piece of information a member of the research group was able to obtain through the SSL Proxying is the pairing ID of a personal PayPal account as shown in Figure 15.

The second transaction was attempted on PayPal and resulted in the same error message as the first attempt. In this attempt however, the error message did not take a minute and thirty seconds to appear, but rather it appeared directly after opening the application. In Charles, the research group was able to observe that after SSL Proxying.

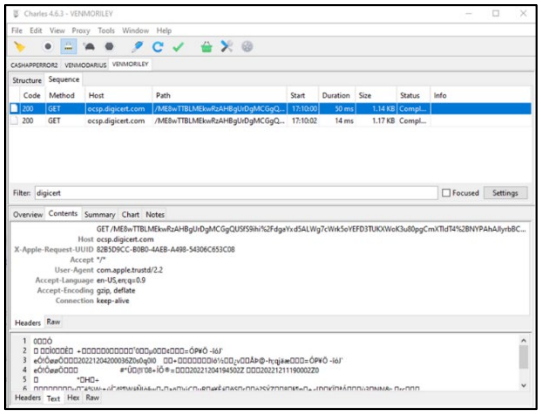

Figure 11: Second Venmo transaction which checked certificate twice and was verified by Venmo.

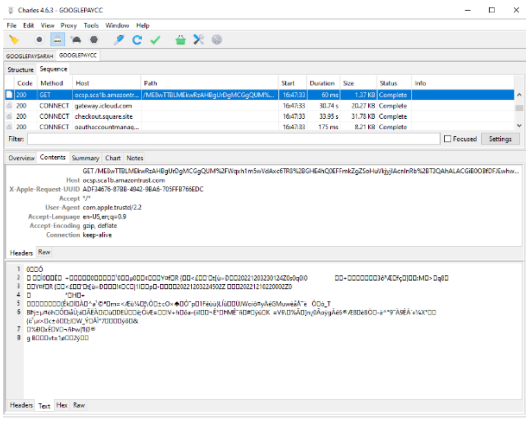

Figure 12: First Google Pay transaction with certificate verified and checked

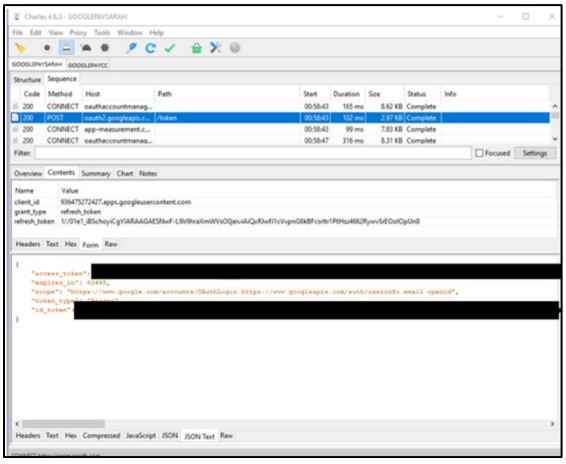

Figure 13: Second Google Pay transaction displaying access token and the token ID.

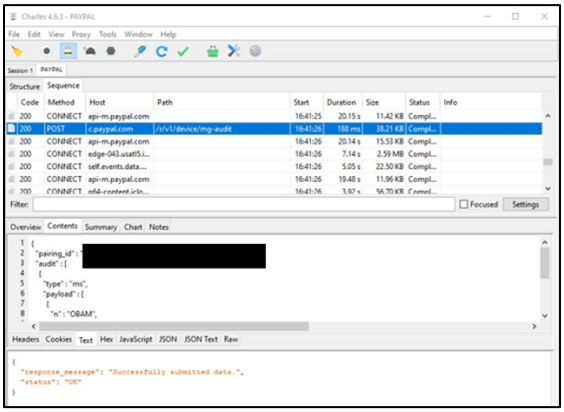

Figure 15: First PayPal transaction displaying pairing ID of personal PayPal account.

| | Apple Pay | Google Pay | Cash App | PayPal | Venmo |
|---|---|---|---|---|---|
| **Detected SSL Proxy** | No | No | Yes | No | No |
| **Verified Digital Certificate** | Yes | Yes | No | No | Yes |

Table 2: Summary of results.

## DISCUSSION AND CONCLUSION

Mobile payments have become the quick and easy way to conduct a transaction in modern times. A comparison of five mobile payment options were highlighted: Apple Pay, Google Pay, Venmo, PayPal, and Cash App. This project explored two potential security scenarios to demonstrate how mobile payment companies could easily gather a customer's personal information.

### Experimental Scenarios Conclusions

In the first scenario, the owner of Collectibles could access a variety of their customer's personal information just from a name and phone number. In this experiment, it is apparent from the results that the owner could potentially sell this information on the Dark Net or utilize it for blackmail. The availability of personal information from simply a phone number should not be as easy as it was found to be through this experimental scenario. Within minutes of research, the owner could dive deeper into a customer's family and create their own database of findings. This is a very real-life possibility and should make the audience aware that sometimes rewards programs are not worth your private information.

The occurrence of the second experimental scenario in the real world is not as likely as the first scenario. Hypothetically, the owner of Collectibles could validate if a random assortment of numbers was a valid card number. However, guessing a customer's number based on just the last four digits could be tricky for someone who the time does not have to sort through potentially thousands of card numbers to find a valid one. Even with just a card number, the owner would not have the expiration date of the card or the CVV (Card Verification Value) of the card. A person's

card number is still a private piece of information even without the CVV or expiration date. This scenario was essentially to show that with algorithms and time, finding a valid card number is a possibility.

**Mobile Payment SSL Proxying Test Conclusions**

For Apple Pay, the expected results varied from what was concluded following the security test. The SSL Proxying was not detected by Apple Pay and allowed for the two transactions to continue. This should be quite a concern to those who utilize Apple Pay. If an unethical hacker can utilize SSL Proxying on a public network, such as a Starbucks, they could potentially see decrypted Apple Pay transactions from anyone who is connected. This problem should be addressed by Apple due to the size of the company and the millions of customers at risk.

For Cash App, the expected results of the two transactions were the results the research group had hoped for concerning the mobile payment option. As soon as the application was launched on the iPhone 7, Cash App realized what was attempting to perform. This shows that with SSL Proxying on, Cash App was able to detect and stop a transaction from occurring, something Apple failed to do. This should make users of Cash App feel even more secure about their mobile payment option. It is also very interesting that Cash App was able to stop the second attempt of a transaction but with a different security error.

For Google Pay, the results were not what was expected, like Apple Pay. Both transactions on Google Pay were able to proceed without any errors or detection of the SSL Proxying. While Google Pay might not be as popular as some of the other options, the security of a user's network traffic is quite important. In the future, it is expected that Google Pay will address this issue/security risk. Google Pay users should be concerned about their network traffic not being as secure as they might initially believe it is. Google is no small company, so for SSL Proxying to not be detected, it was shocking.

For Venmo, the results were like Apple Pay and Google Pay. The two transactions were successfully able to take place and did not show any errors or detections of the SSL Proxying. This should concern the users of Venmo. If an unethical hacker can see a user's network traffic, they could obtain personal information without the user even knowing. This can be seen in Figure 10 where the name and Venmo ID are shown in plain text.

For PayPal, the results were like Cash App in a sense. PayPal was able to turn off the connection from Charles and the iPhone 7, but the network traffic did not specify a validation of a certificate in any portion of the traffic. The researchers found this quite strange and concluded that PayPal detected the SSL Proxying but did not inform Charles that the SSL Proxying was detected. It is also very concerning that the personal information was found so easily in the network traffic while utilizing SSL Proxying and was not even able to access any function of the application on the iPhone 7.

In conclusion, this project covered in depth the five mobile payments discussed and their security measures. Mobile payments are constantly evolving and will always have bugs to follow. These test transactions conclude that people should take their purchasing seriously and monitor their

mobile payment traffic if possible. How people perceive mobile payments in the coming years will determine if it is truly the future of payments. Citizens that utilize mobile payments regularly should be aware of potential security risks that come with purchasing with mobile payments. Even the most used and popular mobile payments are not flawless. When considering using mobile payments, the user should compare the different mobile payments out there to determine which one fits their needs the best. Mobile payments have the power to revolutionize how currency is handled or frighten people away from using it entirely due to security concerns.

## REFERENCES

50+ Global Mobile Payment Stats, Data & Trends. (2022). Retrieved December 4, 2022, from https://www.merchantsavvy.co.uk/mobile-payment-stats-trends/

Ahmed, W., Rasool, A., Javed, A. R., Kumar, N., Gadekallu, T. R., Jalil, Z., & Kryvinska, N. (2021, August 16). Security in Next Generation Mobile Payment Systems: A Comprehensive Survey. IEEE Access, 9, 115932–115950. https://doi.org/10.1109/ACCESS.2021.3105450

Apple Pay. (2022). Apple. Retrieved December 4, 2022, from https://www.apple.com/apple-pay/

Apple Pay component security. (2022, May 13). Apple Support. Retrieved December 4, 2022, from https://support.apple.com/guide/security/apple-pay-component-security-sec2561eb018/web

Apple Pay – statistics and facts. (2022). Statista. Retrieved December 4, 2022, from https://www.statista.com/topics/4322/apple-pay/

Agarwal, S., Qian, W., Ren, Y., Tsai, H. T., & Yeung, B. Y. (2020). The real impact of FinTech: Evidence from mobile payment technology. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3556340

Bankrate (2023, July 1) Credit card fraud statistics. https://www.bankrate.com/finance/credit-cards/credit-card-fraud-statistics/#fraud

Baykara, S. (2022, March 3). What Exactly is PCI DSS Level 1 and What Do its Requirements Entail? PCI DSS GUIDE. https://www.pcidssguide.com/what-exactly-is-pci-dss-level-1-and-what-do-its-requirements-entail/

Birsan, A. (2020, January 8). The Bug That Exposed Your PayPal Password. Medium. https://medium.com/@alex.birsan/the-bug-that-exposed-your-paypal-password-539fc2896da9

Cash App. (2022). App Store. Retrieved December 4, 2022, from https://apps.apple.com/us/app/cash-app/id711923939

Cash App—Save on everyday spending. (2022). Retrieved December 4, 2022, from https://cash.app/spend

COVID-19 Drives Global Surge in use of Digital Payments. (2022, June 29). World Bank. Retrieved December 5, 2022, from https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments

Crypto on Venmo. (2022). Crypto on Venmo. Retrieved December 4, 2022, from https://venmo.com/about/crypto/

Curry, D. (2022, October 25). Mobile Payments App Revenue and Usage Statistics. Business of Apps. https://www.businessofapps.com/data/mobile-payments-app-market/

Curry, D. (2022, September 6). PayPal Revenue and Usage Statistics. Business of Apps. https://www.businessofapps.com/data/paypal-statistics/

Curry, D. (2022, September 6). Venmo Revenue and Usage Statistics. Business of Apps. https://www.businessofapps.com/data/venmo-statistics/

Curry, D. (2022, September 6). Cash App Revenue and Usage Statistics. Business of Apps. https://www.businessofapps.com/data/cash-app-statistics/

Drapkin, A. (2022, December 1). Data Breaches That Have Happened in 2022 So Far—Updated List. Tech.Co. https://tech.co/news/data-breaches-2022-so-far

Find supported payment methods—Google Wallet Help. (2022). Retrieved December 4, 2022, from https://support.google.com/wallet/answer/12059326?visit_id=638051692664203773-4152292388&rd=1

Google Pay Safety & Security Features—Google Safety Center. (2022). Retrieved December 4, 2022, from https://safety.google/pay/

Google Pay: Save and Pay - Apps on Google Play. (2022). Retrieved December 5, 2022, from https://play.google.com/store/apps/details?id=com.google.android.apps.nbu.paisa.user&hl=en&gl=US

Google Pay use per country. (2022, March). *Statista*. Retrieved December 4, 2022, from https://www.statista.com/statistics/1264984/global-google-pay-adoption/

Google Pay—Learn What the Google Pay App Is & How To Use It. (2022). Retrieved December 4, 2022, from https://pay.google.com/about/

HTTP Methods GET vs POST. (2022). Retrieved December 4, 2022, from https://www.w3schools.com/tags/ref_httpmethods.asp

Kauflin, J. (2022, February 2). PayPal Admits 4.5 Million Accounts Were Illegitimate As Fintech's Fraud Problem Grows. Forbes. Retrieved December 4, 2022, from https://www.forbes.com/sites/jeffkauflin/2022/02/02/paypal-admits-45-million-accounts-were-illegitimate-as-fintechs-fraud-problem-grows/

KnowBe4. (2022). Phishing | What Is Phishing? Retrieved December 4, 2022, from https://www.phishing.org/what-is-phishing

Krosofsky, A. (2020, August 25). What Are the Differences Between PayPal and Venmo? Market Realist. https://marketrealist.com/p/does-paypal-own-venmo/

Luhn algorithm. (2022, July 19). GeeksforGeeks. https://www.geeksforgeeks.org/luhn-algorithm/

Mansuri, S. (2022, January 15). Yesterday, today, and tomorrow of mobile payments. Peerbits. Retrieved December 4, 2022, from https://www.peerbits.com/blog/past-present-and-future-of-mobile-payments.html

PayPal Rewards Program | Honey Gold Rewards. (2022). Retrieved December 4, 2022, from https://www.paypal.com/us/webapps/mpp/digital-wallet/ways-to-pay/rewards-points

Public Key Pinning/Certificate pinning. (2022). Cisco Umbrella. Retrieved December 4, 2022, from https://support.umbrella.com/hc/en-us/articles/360030956912-Public-Key-Pinning-Certificate-pinning

Salmon, D. (2019, June 26). I Scraped Millions of Venmo Payments. Your Data Is at Risk. Wired. Retrieved December 4, 2022, from https://www.wired.com/story/i-scraped-millions-of-venmo-payments-your-data-is-at-risk/

Taylor, E. (2016, February 8). Mobile payment technologies in retail: A review of potential benefits and risks. *International Journal of Retail & Distribution Management, 44*(2), 159–177. https://doi.org/10.1108/IJRDM-05-2015-0065

US: Payment methods in retail. (2021). *Statista*. Retrieved December 5, 2022, from https://www.statista.com/statistics/568523/preferred-payment-methods-usa/

Venmo—Share Payments. (2022). Venmo - Share Payments. Retrieved December 4, 2022, from https://venmo.com/

What is a Certificate? (2021, July 6). Retrieved December 5, 2022, from https://www.computerhope.com/jargon/c/certific.htm

What is an Application Programming Interface (API)? | IBM. (2020, August 19). Retrieved December 6, 2022, from https://www.ibm.com/cloud/learn/api

What is a SSL Proxy? Definition & Related FAQs. (2022). Avi Networks. Retrieved December 5, 2022, from https://avinetworks.wpengine.com/glossary/ssl-proxy/

What is Spear Phishing? Definition, Risks and More. (2022). *Fortinet*. Retrieved December 4, 2022, from https://www.fortinet.com/resources/cyberglossary/spear-phishing

Where you can ride transit using Apple Pay. (2022, June 30). Apple Support. Retrieved December 4, 2022, from https://support.apple.com/en-us/HT207958

Xue, J., & Lin, L. (2019). Analysis of the Influence of Mobile Payment on Consumer Behavior. *4th International Conference on Humanities Science and Society Development* (ICHSSD 2019) (pp. 121-127).

# QRBD

# Quarterly Review of Business Disciplines

August 2023

Volume 10
Number 2

A Journal of International Academy of Business Disciplines
Sponsored by University of North Florida
ISSN 2334-0169 (print)
ISSN 2329-5163 (online)