The Security of Venmo in Today's Digital Landscape

Susannah J. Church
Sponsor: Ming Chow

December 2015

Contents

1 Abstract

In today's world, there is a new verb for paying someone back. "You can just venmo me" is commonly heard at coffee stands or over dinner checks. The process of electronically passing money through a mobile phone from person to person feels seamless: a user signs up, adds a bank account or card, and can then send, request, and receive money with the click of a button. Is our technology-minded population unknowingly sacrificing the security of their finances? It's a question many have asked as Venmo's named has graced headlines over security concerns. This paper will look at the security of Venmo in the context of today's mobile world. It will analyze certain aspects of the company's security measures and make recommendations to the company and to its users on how to better protect themselves. Lastly, it will make a judgement on how Venmo is doing compared to other companies in its market and in our digital landscape. Ultimately, this paper will inform Venmo's large user base of the risks they take when they hand over their financial information and discuss improvements for the future.

2 Introduction

2.1 The Rise of Mobile Transfers

2.1.1 What is Venmo?

Venmo is a mobile payment service aimed at making paying friends back easier. Available for iOS, Android and web, the service allows users to send and receive payments by hooking up a bank account, credit or debit card. Transactions can be displayed on your newsfeed for friends to see. When a user creates an account with Venmo, they have access to their contacts on the app, a newsfeed with friends' payment information, and the user's Venmo balance. Money that the user receives from friends will stay in her Venmo balance until she "cashes out" to a bank account, or until the money is used for other payments[1].

2.1.2 Adoption

Founded by two friends in 2009[5], Venmo has rapidly become the face of peer-to-peer mobile payment. In the third quarter of 2015, Venmo processed $2.1 Billion in payments[6]. Venmo's transaction volume has increased by 247% year-over-year[7]. While Venmo does not release statistics on its users, millennials account for about 55% of mobile payment users[8].

2.1.3 Common Uses

According to the Nielson report of 2014, 49% of peer-to-peer transactions are for dining, 36% are for transactions such as household bills, and 19% are for rent[8].

2.2 Venmo's Promise of Security

Venmo has a page dedicated to security on its website. The company boasts bank-grade security systems and discusses its support options. Venmo claims that its product is "inspected and certified by industry leading security experts" and are "meeting or exceeding industry standards and best practices."[2], but only elaborate to say that all financial information is encrypted and stored securely behind firewalls.

2.2.1 Customer Support

For all account-related concerns, Venmo provides an email for support. There is no phone number for customer support offered, and research turned up no phone number that could connect to the company.

2.2.2 Types of PII Stored

According to Venmo's privacy policy[4], Venmo stores the following information about its users:

- Name, telephone number, street address, email address
- Machine/mobile ID, other mobile device information
- Last 4 digits of social security number, date of birth
- Bank account and routing numbers, credit card numbers
- Geo-location

2.3 The Face Behind the Dollar Signs

2.3.1 Ownership

As of 2013, Venmo is owned by PayPal[6]. Founded in 1998, PayPal has worked on many aspects of securing money transfers. Due to its similarity to Venmo, PayPal's pitfalls and triumphs in the security field are relevant to Venmo's growth.

2.3.2 Engineering Team

According to Venmo's website, they have an engineering team of approximately 50, and only one's title is "Security Engineer"[3].

3 To The Community

In college, I have witnessed the rapid adoption of technologies like Venmo first-hand. My generation trusts technology in a way that previous generations have not– in my opinion, often too much and with not enough forethought. It is important for my peers to understand what risks they accept when handing over their personal and financial information to a third-party.

3.1 ”The Internet of Way Too Many Things”

Our culture is constantly immersed in the newest convenient app. Want to find parking? Call a car? Have groceries delivered? There's an app for that. Venmo is not an exception to this rule. It is an app of convenience. It is an app that saves you a couple of minutes in your day. Apps like venmo are trendy right now, and people tend not to think much about the security of what they are doing. In some cases, not having an app like Venmo is an inconvenience, if friends are using it and want their friends to use it too.

4 Security Analysis

4.1 PCI Compliance

Venmo is PCI-compliant[10], which is an important industry standard for maintaining secure systems for payment services. The Payment Card Industry Data Security Standard has six control objectives for compliance with their standard[12]:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Many requirements for these objectives are vague, i.e. ”maintain secure systems”. However, there are a few notable requirements that shed light on Venmo’s implementation of security. The first item, to build and maintain a secure network, requires installing and maintaining a firewall configuration to protect cardholder data. Venmo states on their website that they protect user data with firewalls[2]. In protecting cardholder data, Venmo, as required by PCI, encrypts transmission of cardholder data across open, public networks using TLS 1.2. However, other requirements are fairly obvious and trivial such as changing default passwords for software used and regularly testing systems and processes.

4.2 Encrpytion

4.2.1 Use of TLS

Venmo uses Single Sockets Layer (TLS 1.2) for encryption of communication. The system uses 2048-bit RSA keys for the initial communication of the AES 128-bit encryption key between the client and the server (see Figure 1). These specs are the leading industry standards for using TLS securely[13]. It has been shown that for most uses, the number of bits for AES encryption (128 vs. 256) does not have an effect on the system's security[14], so the choice of 128 bits is acceptable.

4.2.2 Signature Algorithm

Venmo's certificates use a SHA-256 signature algorithm (see Figure 1). SHA1 is being phased out of certificate signing because of its insecurity. As a result, all certificates need to be updated to using SHA-2 algorithms. This is an important move that the industry is hoping to make by 2016, when using SHA-1 will no longer be valid for certificates. Venmo has already updated all of its certificates to reflect the move[13].

4.2.3 Perfect Forward Secrecy

While SSL is the main tool used for securing connections, there are important steps that must be made to use it securely. Perfect forward secrecy ensures that the compromise of a key will only permit access to data of a single key[15]. A necessity for using SSL securely is that the connection has perfect forward secrecy. Venmo uses Elliptic Curve Diffie-Hellman key exchange (see Figure 1), which implements perfect forward secrecy.

4.2.4 HSTS

Venmo uses HTTP Strict Transport Security, which prevents attackers from trying to downgrade the protocol to using HTTP. Venmo requires a connection through HTTPS and will never communicate over HTTP. Venmo also protects against POODLE attacks and virtually all protocol downgrade attacks by using `TLS_FALLBACK_SCSV` in its headers.

4.3 Authentication

Venmo uses OAuth 2.0 to verify users using its API. This opens doors for any vulnerabilities within OAuth itself, which has proven to have security issues[16]. It has been stated that OAuth2.0 is not meant to be used for authentication. Instead, it is an authorization protocol. The difference between the two are distinct- and important[17].

4.3.1 Social Engineering Attacks

After facing criticism earlier this year, Venmo has taken steps to prevent and properly notify a user about a social engineering attack[11]. Two-factor authentication is an important step in social engineering attacks since it will prevent an attacker from getting in with only a stolen password. In addition to two-factor authentication, Venmo added email alerts for any unusual activities happening on an account. A change in password or signing in from a new location are examples of activities that warrant a notification. Venmo offers, but does not require, a 4-digit PIN feature to be used when opening Venmo on your phone[2]. A pin could prevent someone who has a user's physical device and wants to steal funds. These are important measures in the context of a social engineering attack.

4.4 Insurance

4.4.1 FDIC Insurance

The Federal Deposit Insurance Corporation is an institution that provides insurance on deposits under $250,000 dollars in a bank account. FDIC insurance is an important aspect for someone wanting to hold money in an account for an extended period of time because it insures the money to the account owner. In a situation where a bank fails or goes bankrupt, the Federal Depost Insurance Corporation will pay the account holder however much money was in their account within a few days. Thus, the account holder never needs to worry about losing his money due to the banking institution failing[18].

4.4.2 Venmo is a Non-Banking Institution

Under the Federal Deposit Insurance Corporation, Venmo is not considered a bank. Thus, it is not legally required to be FDIC-insured[18]. Many Venmo users choose to have balances on their account so they don't need to pull from their bank account every time they want to make a payment. This decision to not cash-out their balance seems innocent- however, if Venmo were to ever go under, users risk losing their balances or having to go to court to retrieve them from the company.

4.4.3 Google Wallet is FDIC Insured

As of December 2015, funds inside of Google Wallet are now FDIC-insured. Google Wallet was able to make this change because the company will hold the balances of user's accounts in different banking institutions that have FDIC insurance[18]. This is an important step in securing users' money.

4.5 Analysis Results in Context

Venmo has implemented the known industry standards to ensure security against attackers. It protects the data it transmits with the proper encryption and protects the data it stores behind firewalls on secure servers. However, even these reliable systems used across the industry fail and attackers get through. This issue represents larger security flaws in our digital climate.

4.5.1 Social Engineering

Venmo is going to be a larger target of social engineering because of the financial information it handles. The steps Venmo took this year to better secure against social engineering were far too delayed but are now very useful and are important industry standards.

4.5.2 Banking

Google Wallet's decision to be insured by the FDIC was an important one. While the specifics of Google Wallet's security is beyond the scope of this paper, FDIC insurance makes Google Wallet a potentially better choice for users if they like to hold a signifcant balance in their electronic wallets.

4.5.3 Comparison to Online Banking Systems

After reviewing Venmo's encryption system, I decided to do a similar review of my bank's online web system. Venmo's system was slightly more secure than Bank of America's online system. Bank of America had not implemented Forward Secrecy and was using SHA1 encryption for its certificates. Security of a system only means so much without the context of its climate. Despite its flaws, if Venmo is doing better than one of the most widely used banking systems in the United States, it's doing quite well. For further context, please see the supporting material.

5 Action Items

5.1 For Venmo

5.1.1 Customer Support

As a target for social engineering attacks, Venmo needs to be prepared. To start, they need a better system of customer support. While Venmo claims "our support team is the lifeblood of Venmo and we aim to be the biggest advocates for you", if there is no phone number to contact when something goes wrong, the support team is not fully doing their job. In situations where money is involved, people require immediate action. An email does not feel immediate. Implementing higher standards of support will make customers feel safer at night.

5.1.2 Education on Social Engineering

Venmo offers tips on what kinds of triggers to look out for in protecting yourself against social engineering, but it does not do so aggressively enough. There are tips in the security section of its website and on their blog, but there should be consistent reminders communicated in the user experience of the app that will remind users to be vigilant and how to feel out whether something is not right. There are many resources on building a good defense against social engineering.

5.1.3 Become a Bank

It is very difficult to find information on how Venmo handles users' balances. This should be more transparent, and Venmo should use FDIC-insured institutions to store users' balances. This will provide better security, make Venmo a better competitor, and make users' funds more safe.

5.2 For Users

5.2.1 Protect Yourself

As Venmo does its part to protect users against social engineering attacks, users must educate themselves[2]. Use PINs when available, know what social engineering looks like, use distinct passwords, and understand that no system is every perfectly secure.

5.2.2 Manage Your Risk

As a user, you must weigh the pros and cons of releasing your personal information. Is using Venmo worth the risk? Inform yourself on what you're buying into when you download an app, and think about whether it is worth it. For some, it may be. For others, it may not.

6 Conclusion

Venmo has received a lot of criticism this year for its security. While the concerns over lack of two-factor authentication and alerts were valid, the company has remedied those issues. Those missteps do not accurately represent the level of security of Venmo's entire system. As noted, Venmo takes its encryption implementation farther than Bank of America's secure website does. While Venmo cannot be deemed completely ”secure” (as no website can), the company has definitely taken steps to ensure its system puts up a reliable defense. Many people often ask, ”Should I trust a system like Venmo to protect my PII?”. After researching this topic, it seems you can trust Venmo as much as any secure system released today. But I think people need to be asking that question much more– and to institutions they assumed they could trust (like banks). Venmo uses leading security best practices to protect itself. But it's still not enough.

References

[1] Venmo. Web. https://venmo.com/about/product/.

[2] Venmo. Web. https://venmo.com/about/security/.

[3] Venmo. Web. https://venmo.com/team/.

[4] Venmo. Web. https://venmo.com/legal/us-privacy-policy/.

[5] D'Onfro, Jillian. Business Insider. 4 June 2014. Web. http://www.businessinsider.com/venmo-origin-story-facts-andrew-kortina-2014-6.

[6] Reader, Ruth. Venture Beat. 28 October 2015. Web. http://venturebeat.com/2015/10/28/paypal-reveals-how-it-will-finally-cash-in-on-venmo/

[7] Toplin, Jaime and Bakker, Evan. Business Insider. 21 August 2015. Web. http://www.businessinsider.com/venmos-new-segment-and-its-future-2015-8

[8] Nielsen. 10 July 2014. Web. http://www.nielsen.com/us/en/insights/news/2014/whats-in-your-wallet-mobile-payments-are-making-life-easier.html

[9] Sheffield, Brandon. Gamasutra. 20 August 2009. Web. http://www.gamasutra.com/view/feature/132500/dirty_coding_tricks.php?page=1

[10] Vaughan, Michael. Venmo. 27 February 2015. Web. http://blog.venmo.com/hf2t3h4x98p5e13z82pl8j66ngcmry/2015/2/27/a-note-to-our-venmo-community

[11] Pasumarty, Aditya. Venmo. 02 April 2015. Web. http://blog.venmo.com/hf2t3h4x98p5e13z82pl8j66ngcmry/2015/3/30/updates-to-venmo-security

[12] Payment Card Industry Data Security Standard. Requirements and Security Assessment Procedures Version 2.0. Security Standards Council. October 2010. https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

[13] Ristić, Ivan. SSL/TLS Deployment Best Practices. Qualys SSL Labs. Version 1.4. 8 December 2014. https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf

[14] 128-Bit Versus 256-Bit AES Encryption. Seagate. http://www.axantum.com/AxCrypt/etc/seagate128vs256.pdf

[15] RFC 2409 Section 3-3. https://tools.ietf.org/html/rfc2409section-3.3

[16] Sans. Four Attacks on OAuth. How to Secure Your OAuth Implementation. https://www.sans.org/reading-room/whitepapers/application/attacks-secure-oauth-implementation-33644

[17] Richer, Justin. OAuth. User Authentication with OAuth 2.0. http://oauth.net/articles/authentication/

[18] Woodruff, Mandi. Yahoo Finance. 20 April 2015. Web. http://finance.yahoo.com/news/google-wallet-venmo-paypal-fdic-insurance-215842545.html