# MIS 6330 - Spring 2019

## Group Project Milestone 1

### Group 7

Ash Malhotra

My Tra Pham

Sundar Sreenivasan

Suyash Gupta

# Table of Contents

# EXECUTIVE SUMMARY

This report is a risk assessment of the Venmo mobile payment service. It identifies vulnerabilities and threats to the service, resultant risks, and controls to mitigate those risks.

The Venmo service provides two core functions. First, it allows peer-to-peer (P2P) transfers of credit and debit funds via mobile platforms on Android and iOS. Second, it "socializes" these financial transactions by incorporating common social media features such as newsfeeds, timelines, friend requests, commenting, and post-favoriting. The latter function makes Venmo stand out among other mobile payment platforms. Additional features, such as "linking" an individual's Facebook account to Venmo, or finding friends via phone numbers, highlights the centrality of this "socialization" function.

These two functions are supported by the management, operational, and supporting business processes ("Business Process," n.d.). The management processes govern the operation of Venmo's system. This includes the change management process, which drives functional changes to the Venmo platform. It also includes the Business Continuity Plan (BCP) and Disaster Recovery (DR) operations. The operational processes create value for the Venmo service by delivering its core business. It includes procurement processes, which enable access to the software and hardware resources required to make the mobile payment platform a reality. It also includes the Human Resources function, which acquires necessary labor and training to develop, execute and support Venmo. The supporting processes support the core business processes. This includes processes like accounting, to manage finances, and technical support, to manage the IT environment.

Our risk assessment takes an enterprise-wide approach to improve Venmo’s cyber security, ensuring that IT processes and procedures ultimately support Venmo’s business objectives.

# SECURITY EXPECTATIONS & ISSUES

This section first discusses stakeholders’ security expectations of the Venmo mobile payment service. Then, it identifies security-specific issues that can undermine these expectations.

## Security Expectations

There are three main categories of security expectations: physical security, financial security, and data security.

First, there is an expectation that Venmo will invest in physical security to safeguard its business operations. The business needs to make sure that all the information is housed in a suitable data center. The data center needs to be designed such that it can safeguard against threats like natural disasters, power outages, and unauthorized personnel access. The business also needs to invest in reliable physical IT infrastructure, like network devices and servers, which supports business operations without compromising the confidentiality, integrity, and availability of Venmo’s assets.

Second, there is an expectation that Venmo will invest in financial security. Given that Venmo’s core function is the P2P transfer of funds, financial security is critical to the survival of the business. This includes following regulatory requirements and using tools to secure payments. Venmo only operates within the United States, however there is no single law or legal authority that governs the mobile payment landscape (Crowe, Keppler, & Merritt, 2012). As a result, Venmo needs to invest in meeting a patchwork of regulatory and compliance requirements across multiple agencies, like the Office of the Comptroller of the Currency (OCC) or the Federal Communications

Commission (FCC). The use of physical financial tools, like the Venmo Mastercard, and digital tools, like the Venmo Wallet, necessitate hardware and software controls to protect financial data. These controls include (but are not limited to) digital wallet encryption and credit card chip technology. The goals are to secure consumers' finances while they are using the Venmo service.

Third, there is an expectation of data security to protect the intangible assets that facilitate core business functions. The data assets include personally identifiable information (PII), like users' IP addresses and phone numbers. Such assets also include other personal information, like users' location, number of transactions, purpose of transactions, friend networks etc. The business needs to invest in network security, ensuring that privacy controls and data processes provide a level of confidentiality, integrity and availability that is fair to consumers. This expectation is especially important given the "social" character of the Venmo platform.

## Security-Specific Issues

There are several security issues posed by the Venmo service, and they impact all three areas of stakeholders' security expectations. This section identifies four key issues.

First, Venmo risks exposing personal information by using a publicly configured Application Programming Interface (API). A publicly configured API is a vulnerability that can compromise the confidentiality of consumers' personal data. It is possible to view the public API endpoint, execute a GET request, and begin "scraping" transaction data from P2P interactions on the application (Matsakis, 2018). The result is that the data from hundreds of thousands of transactions can be downloaded every day. A variety of threats are capable of exploiting this vulnerability. A malicious actor can download users' financial activity and use it to track or target individual users across the United States. Bots can be used to skim this data at scale and track the nature and location of people's activities. The outcome i.e. risk is a violation of consumer privacy as the confidentiality of users' financial activity is compromised. This undermines data security expectations of the Venmo service.

Second, social media features expose the privacy of users. Social media features on Venmo include required commenting/posting for every P2P transaction, names of users involved in a transaction, and even a timeline showing a users' history of transactions. By default, Venmo privacy options are turned off, leaving users' personal data publicly available. The open social media features are a vulnerability for the system that can be exploited by multiple threats. A malicious actor can view a user's closest friends, the time and date of transactions, and the specific types of goods and services purchased. Comments under every transaction-post even provide language specific content. The most relevant, immediate threat is a spear-phishing attack (Salmon, 2019). It is easy to combine this publicly available data to target unsuspecting users. For example, two friends may Venmo each other for movie tickets on a regular basis. A malicious actor could email one of those friends a deceptive email that includes an attachment for "tickets," in the process delivering malware that gains unauthorized access to user information. The risks range from identity theft to financial theft, depending on the success of Venmo-based spear-phishing campaigns. It is also possible for a malicious actor to "spoof" a payment recipient by copying the profile picture and name of individuals. This increases the chance of payments being sent to the wrong person. Ultimately, this social media/privacy vulnerability can undermine the data security and financial security expectations of the Venmo service.

The first and second security issues relate to users' personal information. By exploiting both of these vulnerabilities, malicious actors can follow users' personal lives to an alarming level of detail and launch a variety of attacks. Privacy advocate Hang Do Thi Duc developed the website Public By Default (https://publicbydefault.fyi/) to showcase how the public API information and social media information can be combined to develop detailed profiles on users (2018). In one of her case studies, she was able to follow two users' entire romantic relationship from the beginning to the end, complete with office names, work schedule, and phone numbers– all drawn from a combination of Venmo comments and API data scraping (Do Thi Duc, 2018). The main point is that the first two security issues are the most problematic for the Venmo platform, as they compromise personal information and make users susceptible to a multitude of cyber threats.

Third, Venmo's use of mobile systems poses a challenge for account security. Specifically, the use of a mobile one-time password (OTP) delivered via SMS, to log into an account is an exploit. The threat is a SIM Swap, which occurs when a malicious actor uses social engineering to convince a mobile service provider to switch a customer's number over to a new SIM, usually on a new device (Andrews, 2018). This threat can help an actor exploit the texted-OTP vulnerability to gain access to a user's Venmo account. The risk is financial theft, as malicious actors can empty out Venmo wallets or draw Venmo transfers from users' debit or credit cards. This vulnerability undermines the financial security and data security expectations of the Venmo service.

Fourth, Venmo's reliance on physical IT infrastructure poses some inherent security challenges. Vulnerabilities exist throughout the infrastructure, from the physical security of data centers where information is stored to the reliability of networks that Venmo employees use to access the application. Threats that exploit these vulnerabilities include events like natural disasters, fires, and network outages. The associated risks include the loss of consumer data and the loss of application accessibility. Vulnerabilities in the physical IT infrastructure can undermine physical security and data security expectations of the Venmo service.

# HIGH-LEVEL SECURITY REQUIREMENTS

Venmo needs to develop internal and external controls that meet regulatory compliance standards. Considering that Venmo operates only in the United States, the service only needs to worry about meeting policies in the US for financial corporations. By meeting critical laws, regulations and standards governing the financial technologies sector, Venmo can systematically mitigate its security risks.

First, Venmo needs to comply with laws such as the Gramm-Leach-Bliley (GLB) Act. As the Federal Trade Commission (FTC) explains, the GLB Act "requires financial institutions… to explain their information-sharing practices to their customers and to safeguard sensitive data" ("Gramm Leach Bliley Act," n.d.). This includes Personally Identifiable Information (PII), such as financial accounts, email addresses, and phone numbers. Compliance with this law directly supports data security and financial security expectations.

Second, Venmo needs to comply with regulations governing internal controls and financial activity. Specifically, it should comply with the 2002 Sarbanes Oxley Act (SOX) and the Federal Financial Institutions Examination Council's (FFIEC) regulations. SOX mandates, among other requirements, the need for effective IT controls that manage financial processes (Hall, 2016). SOX is particularly relevant to Venmo given its handling of customer financial account data. The FFIEC is important because it provides uniform regulatory guidance for financial companies to meet the requirements of five different US regulatory authorities: the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Association (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) ("About the FFIEC," n.d.). In other words, Venmo can meet a multitude of different regulatory requirements by following guidance from the FFIEC. Regulatory compliance with SOX and the FFIEC supports physical security, data security and financial security expectations.

Third, Venmo needs to comply with industry standards that safeguard the management of information. Specifically, it must comply with the Payment Card Industry Data Security Standards (PCI-DSS) and the ISO 27001 standards. A 2011 study found that 64% of PCI-DSS compliant firms experienced no security breaches that endangered credit card information, compared to a 34% rate for non-compliant firms (“PCI DSS Appears to Reduce Breaches,” 2011). Since Venmo handles users’ credit card and debit card information in order to enable payments, PCI-DSS compliance reduces the risk of financial data breaches. The result is greater trust in the Venmo mobile payment service. Venmo also needs to implement Information Security Management Systems (ISMS) in order manage risk and safeguard information while meeting its business objectives. The ISO 27001 is a group of standards for implementing an ISMS within a business (Matarocioglu, 2011). Venmo’s use of ISO 27001 standards will help it mitigate risks and apply safeguards systematically and efficiently. Compliance with industry standards like PCI-DSS and ISO 27001 supports data security and financial security expectations.

This report includes a risk matrix in the **accompanying spreadsheet**. It identifies important threats and performs a risk assessment. The assessment recognizes various controls that can mitigate risks to the Venmo service and support a higher level of security for the business.

# KEY SECURITY ROLES

In response to the rise of cyber risk, effective risk management empowers Venmo's management to protect customers from security threats. There are three lines of defense: business and IT functions (1st line of defense), information and technology risk management functions (2nd line of defense) and internal audit (3rd line of defense) ("Cybersecurity - The Role of Internal Audit," 2015). Internal auditors play a critical role in assessing risks and identifying opportunities to strengthen security. They are responsible for independently reviewing the effectiveness and efficiency of the internal controls to ensure the controls mitigate risks posed by cyber threats. They also acquire continuing professional education (CPE) to stay up to date on evolving threats, understand current cyber risks, and address concerns by the audit committee and the board of directors regarding risk management effectiveness ("Cybersecurity - The Role of Internal Audit," 2015).

Besides an effective strategy of risk management, securing networks and systems is one of the most essential tasks for Venmo. Network security engineers enable Venmo to accomplish this by planning, designing, optimizing, and troubleshooting problems to safeguard network security systems and improve the efficiency of the organization (FE Administrator, 2017). As part of the IT function, they protect the network from threats such as cyber-attacks, intrusion, infiltration, and prevent service disruptions due to natural disasters. Testing and simulating emergency scenarios can help avoid a system crash due to these threats. These include, but are not limited to identifying vulnerabilities within a network, maintaining firewalls, web protocols and email security, creating virus and threat detection systems to make sure the network system can bounce back in the event of an attack (FE Administrator, 2017). Network security engineers can collaborate with internal auditors in preventing cyber risks, collecting incident responses when an attack occurs, and investigating hacking incidents.

Another key security role is the Chief Information Security Officer (CISO), the executive who is responsible for Venmo’s information and data security. With an extensive understanding and expertise in network security, the CISO analyzes immediate threats, helps the board understand potential security issues that relate to business decisions, and prevents data from being misused or stolen by internal employees (Fruhlinger, 2019). The CISO is also in charge of identity and access management (IAM), program management, governance, investigations and forensics. This role not only provides an IT executive to work directly with management, but it also provides oversight over security architecture to make sure that IT and network infrastructure is designed using the best security practices (Fruhlinger, 2019).

# KEY STAKEHOLDERS

Cyber risks can be prevented or mitigated if key stakeholders possess a common understanding of security requirements. There are several stakeholders of Venmo that have a direct relationship with the impacts of cyber threats.

First, shareholders are stakeholders who are financially affected by Venmo’s performance. They need to stay updated of cyber risks and controls, as their financial support depends on the success and reliability of the company. Since IT systems must ultimately support business objectives, it is important that shareholders understand how cybersecurity investments improve their bottom line.

Second, executive leadership is a key stakeholder in Venmo’s business because of its responsibility for managing risks. The responsibility to prevent security threats falls not only on IT employees, but also on upper management and the board of directors. They need to be engaged in this risk management process. Management is responsible for providing and pursuing strategies to effectively manage cyber risks. It needs to abide by rules and regulations, such as PCI-DSS and SOX, to make appropriate business decisions that protect sensitive financial information. The board of directors needs to make sure upper management is operating Venmo securely, meeting requirements like internal audit standards, and maximizing shareholder value.

Third, Venmo employees are direct stakeholders who have an interest in mitigating the risks of cyber threats. Employees include such departments as human resources, operations, and legal and compliance. A minor error by human resources can increase the likelihood of “spear phishing” attacks that target specific employees (Reagan, 2015). A cyber incident’s impact on operations can cause the company to slow down or shut down entirely, leading to a wide range of operations costs. Lawsuits also usually follow cyber incidents. Thus, the legal and compliance team are liable for preventing and responding to incidents.

Fourth, customers are key stakeholders because they are trusting Venmo with their individual data. Individual data and privacy protections can be difficult to manage and protect, which makes addressing weak points in Venmo's cyber defenses a top priority (Reagan, 2015). Customers should understand how they can protect their own privacy, personal and financial data. On the other hand, Venmo should implement solutions to better secure customers' data while also preparing effective responses to potential cyber-attacks.

# REFERENCES

About the FFIEC. (n.d.). Retrieved from https://www.ffiec.gov/about.htm.

Andrews, Nathanael. (Jan. 2018). ‘Can I Get Your Digits?’: Illegal Acquisition of Wireless Phone Numbers for SIM-Swap Attacks and Wireless Provider Liability. *Northwestern Journal of Technology and Intellectual Property, 16(2),* 79-105.

Business Process. (n.d.). Retrieved from https://www.techopedia.com/definition/1168/business-process.

Crowe, Marianne, Mary Kepler and Cynthia Merritt. (25 July 2012). The US Regulatory Landscape for Mobile Payments. *Federal Reserve Bank of Atlanta*. Retrieved from https://www.frbatlanta.org/-/media/Documents/rprf/rprf_pubs/120730wp.pdf

Cybersecurity - The Role of Internal Audit [PDF Document]. (2015). Retrieved from https://chapters.theiia.org/Orange%20County/IIA%20OC%20Presentation%20Downloads/2015-08-%20Cyber%20IA.pdf

Do Thi Duc, Hang. (2017). The Lovers. Retrieved from https://publicbydefault.fyi/

FE Administrator. (2017). Network Security Engineer Job Description. Retrieved from https://www.fieldengineer.com/blogs/network-security-engineer-job

Fruhlinger, J. (2019, January 14). What is a CISO? Responsibilities and Requirements for this Vital Role. Retrieved from https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html

Gramm Leach Bliley Act. (n.d.). Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

Hall, James A. (2016). *Information Technology Auditing* (4th ed.). Boston, MA: Lehigh University.

Mataracioglu, Tolga, and Sevgi Ozkan. (2011). *Governing Information Security in Conjunction with COBIT and ISO 27001.*

Matsakis, Louise. (26 August 2018). It's Time to Stop Spending Money on Venmo. Retrieved from https://www.wired.com/story/venmo-alternatives/

PCI DSS Appears to Reduce Breaches. *Computer Fraud & Security, 2011(5)*, 3–19. doi: https://doi.org/10.1016/S1361-3723(11)70047-1

Reagan, Thomas. (25 September 2015). 7 Cyber Risk Stakeholders and Why They Matter. Retrieved from https://www.propertycasualty360.com/2015/09/25/7-cyber-risk-stakeholders-and-why-they-matter/?slreturn=20200030232341

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