DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N. Y. 10013
(212) 335-9000

ALVIN L. BRAGG, JR.
DISTRICT ATTORNEY

January 22, 2024

Brian Grassadonia
Chief Executive Officer
Cash App
16552 North 90th Street, Suite 100
Scottsdale, AZ 85260

Dear Mr. Grassadonia:

I am writing in my capacity as the Manhattan District Attorney in response to a growing number of incidents in the New York City region involving fraud and theft through the exploitation of your company's mobile financial applications on personal electronic devices such as iPhones. These crimes involve an unauthorized user gaining access to unlocked devices and then draining bank accounts of significant sums of money, making purchases with mobile financial applications, and using financial information from the applications to open new accounts. Offenders also take over the phone's security by changing passwords, recovery accounts, and application settings. The ease with which offenders can collect five- and even six-figure windfalls in a matter of minutes is incentivizing a large number of individuals to commit these crimes, which are creating serious financial, and in some cases physical, harm to our residents. While my office, along with the NYPD, investigates and prosecutes these crimes, it is imperative that your company take further action to protect its customers from fraud and theft by adopting additional security measures to deter this illegal activity both locally and across the country.

The use of peer-to-peer payment services has grown exponentially over the past five years, nearing almost $1 trillion in payments across the most-used applications. As these payment networks have become ubiquitous, frauds and scams have proliferated, with fraud claims tripling between 2020 and 2022, costing consumers hundreds of millions of dollars each year.[1] While cash apps, like Cash App, offer consumers an easy and fast method to transfer funds, they also have made these platforms a favorite of fraudsters because consumers have no option to cancel transactions, even moments after authorizing them. I am concerned about the troubling rise in illegal behavior that has developed because of insufficient security measures connected with your software and business policy decisions.[2]

In New York City, cash app frauds have been perpetrated in a variety of different ways. In some instances, the fraudster asks to use an individual's smartphone for personal use, and then quickly sends large amounts of money to themselves through the victim's financial application. In other instances, the offender asks for a donation for a specific cause, offers to transfer the money directly from the victim's smartphone, and then

---

[1] United States Congress, Senate, Banking, Housing, and Urban Affairs Committee, Senator Elizabeth Warren. "Letters to Banks re Zelle." July 7th, 2022.
[2] United States Congress, Senate, Banking, Housing, and Urban Affairs Committee, Senator Elizabeth Warren. "Letters to Banks re Zelle." July 7th, 2022.

transfers significant funds to the fraudster's own account. In the most disturbing cases, offenders have violently assaulted or drugged victims, and either compelled them to provide a password for a device or used biometric ID to open the victim's phone before transferring money once the individual is incapacitated. In all of these cases, we believe further security measures to prevent unauthorized access to unlimited use of your financial services would have prevented such crimes.

Furthermore, the problem is not specific to New York City, as we are seeing increased reports of similar cash app thefts occurring in cities across the United States. Just in the past year, there have been thefts stretching from Los Angeles, where several people were robbed of thousands of dollars through Venmo at knife point, to Orlando, where a woman had thousands drained from her Venmo after a child asked to use her phone. Similar thefts and robberies have been publicly reported in West Virginia, Louisiana, Illinois, Kansas, Tennessee, Virginia and elsewhere across the United States.

To address these alarming incidents, Apple has recently developed 'Stolen Device Protection,' a new feature that creates a second layer of security, making it harder for perpetrators to use a phone's passcode to steal funds when the user's phone is not at home or at work. According to news reports, if the phone is at a location that is not usually associated with its owner, and Stolen Device Protection is turned on, the device will require Apple's FaceID facial recognition in addition to a passcode in order for users to perform sensitive actions, such as viewing stored passwords or wiping the phone. In addition, thieves will not be able to change the user's Apple ID password or remove FaceID without a mandatory one-hour delay.[3] The new software is reportedly in beta testing, with the expectation that it will be more widely available to iPhone users later this year.

In order to protect your customers and our residents, and to reduce how lucrative these thefts currently are, I urge that you implement similar additional security features as a default standard for all users of your product, such as:

1) Add a second and separate password for accessing the app on a smartphone as a default security option. While users may still have the option to turn off the additional security in their settings, multi-factor authentication establishes an extra level of security and should be the standard to protect consumers.

2) Impose default lower limits on the monetary amount of total daily transfers. Transaction limits would reduce the amount of money that can be stolen from a user if a theft occurs, and reduce the incentive for offenders to steal unlocked devices.

3) Require wait times and secondary verification of up to a day for large monetary transactions. This would give the user time to cancel large transactions that were made without their permission and reduce the chances of theft of large amounts of money at one time.

4) Better monitor accounts for unusual transfer activities and ask for confirmation when suspicious transactions occur (e.g. unusually large monetary transactions, monetary transactions late at night, etc.). Similar to the policies of most credit card companies, this would add an extra layer of security to your product to prevent fraudulent transactions.

A failure to take proactive steps in the name of your consumers will lead to further illegal behavior and countless unsuspecting victims.

---

[3] Kif Leswing, "Apple introduces new Iphone security mode to protect against stolen passcodes," CNBC, December 12, 2023, https://www.cnbc.com/2023/12/12/apple-introduces-stolen-device-protection-mode-to-prevent-iphone-theft.html.

Your company has made representations regarding the security and safety of its product for its customers. Cash App claims on its website that it is "a safe space for you and your money." To live up to those representations, more safeguards, like ones now being tested by Apple, are needed to deter theft and protect the personal and financial safety of your consumers.

To that end, I respectfully request a meeting with representatives from Cash App to discuss the steps you are taking to combat this growing concern. My office is committed to working with your company to help develop a comprehensive approach to discourage theft, protect consumers, and fulfill your expressed commitments to public safety.

Respectfully,

Alvin L. Bragg, Jr.
District Attorney

DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N. Y. 10013
(212) 335-9000

ALVIN L. BRAGG, JR.
DISTRICT ATTORNEY

January 22, 2024

Alex Chriss
President and Chief Executive Officer
PayPal Holdings, Inc.
2211 N 1st Street
San Jose, CA 95131

Dear Mr. Chriss:

I am writing in my capacity as the Manhattan District Attorney in response to a growing number of incidents in the New York City region involving fraud and theft through the exploitation of your company's mobile financial applications on personal electronic devices such as iPhones. These crimes involve an unauthorized user gaining access to unlocked devices and then draining bank accounts of significant sums of money, making purchases with mobile financial applications, and using financial information from the applications to open new accounts. Offenders also take over the phone's security by changing passwords, recovery accounts, and application settings. The ease with which offenders can collect five- and even six-figure windfalls in a matter of minutes is incentivizing a large number of individuals to commit these crimes, which are creating serious financial, and in some cases physical, harm to our residents. While my office, along with the NYPD, investigates and prosecutes these crimes, it is imperative that your company take further action to protect its customers from fraud and theft by adopting additional security measures to deter this illegal activity both locally and across the country.

The use of peer-to-peer payment services has grown exponentially over the past five years, nearing almost $1 trillion in payments across the most-used applications. As these payment networks have become ubiquitous, frauds and scams have proliferated, with fraud claims tripling between 2020 and 2022, costing consumers hundreds of millions of dollars each year.[1] While cash apps, like PayPal and Venmo, offer consumers an easy and fast method to transfer funds, they also have made these platforms a favorite of fraudsters because consumers have no option to cancel transactions, even moments after authorizing them. I am concerned about the troubling rise in illegal behavior that has developed because of insufficient security measures connected with your software and business policy decisions.[2]

In New York City, cash app frauds have been perpetrated in a variety of different ways. In some instances, the fraudster asks to use an individual's smartphone for personal use, and then quickly sends large amounts of money to themselves through the victim's financial application. In other instances, the offender asks for a donation for a specific cause, offers to transfer the money directly from the victim's smartphone, and then

[1] United States Congress, Senate, Banking, Housing, and Urban Affairs Committee, Senator Elizabeth Warren. "Letters to Banks re Zelle." July 7th, 2022.
[2] United States Congress, Senate, Banking, Housing, and Urban Affairs Committee, Senator Elizabeth Warren. "Letters to Banks re Zelle." July 7th, 2022.

transfers significant funds to the fraudster's own account. In the most disturbing cases, offenders have violently assaulted or drugged victims, and either compelled them to provide a password for a device or used biometric ID to open the victim's phone before transferring money once the individual is incapacitated. In all of these cases, we believe further security measures to prevent unauthorized access to unlimited use of your financial services would have prevented such crimes.

Furthermore, the problem is not specific to New York City, as we are seeing increased reports of similar cash app thefts occurring in cities across the United States. Just in the past year, there have been thefts stretching from Los Angeles, where several people were robbed of thousands of dollars through Venmo at knife point, to Orlando, where a woman had thousands drained from her Venmo after a child asked to use her phone. Similar thefts and robberies have been publicly reported in West Virginia, Louisiana, Illinois, Kansas, Tennessee, Virginia and elsewhere across the United States.

To address these alarming incidents, Apple has recently developed 'Stolen Device Protection,' a new feature that creates a second layer of security, making it harder for perpetrators to use a phone's passcode to steal funds when the user's phone is not at home or at work. According to news reports, if the phone is at a location that is not usually associated with its owner, and Stolen Device Protection is turned on, the device will require Apple's FaceID facial recognition in addition to a passcode in order for users to perform sensitive actions, such as viewing stored passwords or wiping the phone. In addition, thieves will not be able to change the user's Apple ID password or remove FaceID without a mandatory one-hour delay.[3] The new software is reportedly in beta testing, with the expectation that it will be more widely available to iPhone users later this year.

In order to protect your customers and our residents, and to reduce how lucrative these thefts currently are, I urge that you implement similar additional security features as a default standard for all users of your product, such as:

1) Add a second and separate password for accessing the app on a smartphone as a default security option. While users may still have the option to turn off the additional security in their settings, multi-factor authentication establishes an extra level of security and should be the standard to protect consumers.

2) Impose default lower limits on the monetary amount of total daily transfers. Transaction limits would reduce the amount of money that can be stolen from a user if a theft occurs, and reduce the incentive for offenders to steal unlocked devices.

3) Require wait times and secondary verification of up to a day for large monetary transactions. This would give the user time to cancel large transactions that were made without their permission and reduce the chances of theft of large amounts of money at one time.

4) Better monitor accounts for unusual transfer activities and ask for confirmation when suspicious transactions occur (e.g. unusually large monetary transactions, monetary transactions late at night, etc.). Similar to the policies of most credit card companies, this would add an extra layer of security to your product to prevent fraudulent transactions.

A failure to take proactive steps in the name of your consumers will lead to further illegal behavior and countless unsuspecting victims.

---

[3] Kif Leswing, "Apple introduces new Iphone security mode to protect against stolen passcodes," CNBC, December 12, 2023, https://www.cnbc.com/2023/12/12/apple-introduces-stolen-device-protection-mode-to-prevent-iphone-theft.html.

Your company has made representations regarding the security and safety of its product for its customers. When an individual looks up the Venmo app in the app store, it claims that "Venmo is the fast, safe, social way to pay and get paid." To live up to those representations, more safeguards, like ones now being tested by Apple, are needed to deter theft and protect the personal and financial safety of your consumers.

To that end, I respectfully request a meeting with representatives from your company to discuss the steps you are taking to combat this growing concern. My office is committed to working with your company to help develop a comprehensive approach to discourage theft, protect consumers, and fulfill your expressed commitments to public safety.

Respectfully,

Alvin L. Bragg, Jr.
District Attorney

DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N. Y. 10013
(212) 335-9000

ALVIN L. BRAGG, JR.
DISTRICT ATTORNEY

January 22, 2024

Cameron Fowler
Chief Executive Officer
Early Warning Services, LLC
16552 North 90th Street, Suite 100
Scottsdale, AZ 85260

Dear Mr. Fowler:

I am writing in my capacity as the Manhattan District Attorney in response to a growing number of incidents in the New York City region involving fraud and theft through the exploitation of your company's mobile financial applications on personal electronic devices such as iPhones. These crimes involve an unauthorized user gaining access to unlocked devices and then draining bank accounts of significant sums of money, making purchases with mobile financial applications, and using financial information from the applications to open new accounts. Offenders also take over the phone's security by changing passwords, recovery accounts, and application settings. The ease with which offenders can collect five- and even six-figure windfalls in a matter of minutes is incentivizing a large number of individuals to commit these crimes, which are creating serious financial, and in some cases physical, harm to our residents. While my office, along with the NYPD, investigates and prosecutes these crimes, it is imperative that your company take further action to protect its customers from fraud and theft by adopting additional security measures to deter this illegal activity both locally and across the country.

The use of peer-to-peer payment services has grown exponentially over the past five years, nearing almost $1 trillion in payments across the most-used applications. As these payment networks have become ubiquitous, frauds and scams have proliferated, with fraud claims tripling between 2020 and 2022, costing consumers hundreds of millions of dollars each year.[1] While cash apps, like Zelle, offer consumers an easy and fast method to transfer funds, they also have made these platforms a favorite of fraudsters because consumers have no option to cancel transactions, even moments after authorizing them. I am concerned about the troubling rise in illegal behavior that has developed because of insufficient security measures connected with your software and business policy decisions.[2]

In New York City, cash app frauds have been perpetrated in a variety of different ways. In some instances, the fraudster asks to use an individual's smartphone for personal use, and then quickly sends large amounts of money to themselves through the victim's financial application. In other instances, the offender asks for a donation for a specific cause, offers to transfer the money directly from the victim's smartphone, and then

---

[1] United States Congress, Senate, Banking, Housing, and Urban Affairs Committee, Senator Elizabeth Warren. "Letters to Banks re Zelle." July 7th, 2022.
[2] United States Congress, Senate, Banking, Housing, and Urban Affairs Committee, Senator Elizabeth Warren. "Letters to Banks re Zelle." July 7th, 2022.

transfers significant funds to the fraudster's own account. In the most disturbing cases, offenders have violently assaulted or drugged victims, and either compelled them to provide a password for a device or used biometric ID to open the victim's phone before transferring money once the individual is incapacitated. In all of these cases, we believe further security measures to prevent unauthorized access to unlimited use of your financial services would have prevented such crimes.

Furthermore, the problem is not specific to New York City, as we are seeing increased reports of similar cash app thefts occurring in cities across the United States. Just in the past year, there have been thefts stretching from Los Angeles, where several people were robbed of thousands of dollars through Venmo at knife point, to Orlando, where a woman had thousands drained from her Venmo after a child asked to use her phone. Similar thefts and robberies have been publicly reported in West Virginia, Louisiana, Illinois, Kansas, Tennessee, Virginia and elsewhere across the United States.

To address these alarming incidents, Apple has recently developed 'Stolen Device Protection,' a new feature that creates a second layer of security, making it harder for perpetrators to use a phone's passcode to steal funds when the user's phone is not at home or at work. According to news reports, if the phone is at a location that is not usually associated with its owner, and Stolen Device Protection is turned on, the device will require Apple's FaceID facial recognition in addition to a passcode in order for users to perform sensitive actions, such as viewing stored passwords or wiping the phone. In addition, thieves will not be able to change the user's Apple ID password or remove FaceID without a mandatory one-hour delay.[3] The new software is reportedly in beta testing, with the expectation that it will be more widely available to iPhone users later this year.

In order to protect your customers and our residents, and to reduce how lucrative these thefts currently are, I urge that you implement similar additional security features as a default standard for all users of your product, such as:

1) Add a second and separate password for accessing the app on a smartphone as a default security option. While users may still have the option to turn off the additional security in their settings, multi-factor authentication establishes an extra level of security and should be the standard to protect consumers.

2) Impose default lower limits on the monetary amount of total daily transfers. Transaction limits would reduce the amount of money that can be stolen from a user if a theft occurs, and reduce the incentive for offenders to steal unlocked devices.

3) Require wait times and secondary verification of up to a day for large monetary transactions. This would give the user time to cancel large transactions that were made without their permission and reduce the chances of theft of large amounts of money at one time.

4) Better monitor accounts for unusual transfer activities and ask for confirmation when suspicious transactions occur (e.g. unusually large monetary transactions, monetary transactions late at night, etc.). Similar to the policies of most credit card companies, this would add an extra layer of security to your product to prevent fraudulent transactions.

A failure to take proactive steps in the name of your consumers will lead to further illegal behavior and countless unsuspecting victims.

---

[3] Kif Leswing, "Apple introduces new Iphone security mode to protect against stolen passcodes," CNBC, December 12, 2023, https://www.cnbc.com/2023/12/12/apple-introduces-stolen-device-protection-mode-to-prevent-iphone-theft.html.

Your company has made representations regarding the security and safety of its product for its customers. Zelle claims it is "A fast, safe easy way to send money to friends and family." To live up to those representations, more safeguards, like ones now being tested by Apple, are needed to deter theft and protect the personal and financial safety of your consumers.

To that end, I respectfully request a meeting with representatives from your company to discuss the steps you are taking to combat this growing concern. My office is committed to working with your company to help develop a comprehensive approach to discourage theft, protect consumers, and fulfill your expressed commitments to public safety.

Respectfully,

Alvin L. Bragg, Jr.
District Attorney