JPMORGAN CHASE & CO.

September 22, 2022

The Honorable Robert Menendez
528 Hart Senate Office Building
Washington, DC 20510

The Honorable Jack Reed
728 Hart Senate Office Building
Washington, DC 20510

The Honorable Chris Van Hollen
110 Hart Senate Office Building
Washington, DC 20510

The Honorable Bernie Sanders
332 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Elizabeth Warren
309 Hart Senate Office Building
Washington, DC 20510

The Honorable Sherrod Brown
503 Hart Senate Office Building
Washington, DC 20510

The Honorable Sheldon Whitehouse
530 Hart Senate Office Building
Washington, DC 20510

The Honorable Tammy Duckworth
524 Hart Senate Office Building
Washington, DC 20510

Dear Senator Menendez, Senator Warren, Senator Reed, Senator Brown, Senator Van Hollen, Senator Whitehouse, Senator Sanders and Senator Duckworth:

As I said in my previous letter to you, we invest significantly to protect our customers from fraud; in fact, we stop more than $5 billion in fraud attempts each year across all payment platforms. We are also focused on helping our customers avoid scams – a heartbreaking, decades old form of crime where bad actors prey upon vulnerable Americans, tricking them into paying with cash, checks, wire transfers, cryptocurrencies, gift cards or more recently peer-to-peer payment platforms.

On the Zelle network specifically, more than 99.9% of all transactions are authorized by the consumer and both fraud rates and overall fraud have decreased over time due to fraud prevention and detection techniques implemented by banks like Chase. Chase Zelle also has lower non-fraud claim rates than other payment products like debit and credit card. Consistent with industry reports that fraud and scam dispute rates are 3-6x higher on some other major P2P networks than Zelle, we also observe far higher combined fraud and scam rates on those networks.

At Chase, our financial crimes and cybersecurity experts work to identify patterns and other markers where scams are more likely to occur and invest significant resources to help our customers avoid becoming a victim. When bad actors are detected, Zelle's participant institutions restrict access to Zelle and report the transaction to the network for further monitoring and action. We reimburse customers for unauthorized transactions reported in a timely manner. For 2022, we reimbursed an average of $1.7 million each month for unauthorized payments.

Unfortunately, the industry has seen a number of scams involving bad actors impersonating a bank representative and deceiving customers into sending money via Zelle. The bad actor contacts the customer claiming to be helping resolve fraud on the account and ask the customer to send money "to themselves." The customer is then tricked into providing access credentials – like a one-time passcode – to the bad actor who then registers the customer's email or phone number as their own in a different account. The customer then sends money to their own email or phone number, not realizing that these are

now tied to a bad actor's account. Chase reimburses customers for this type of "me-to-me" scam involving tokens, even though this would be considered an authorized transaction under Regulation E. We also prominently remind customers, in the Zelle experience, that Chase will never contact them asking them to send themselves money.

These are serious issues requiring collaboration between business, government, and law enforcement to address. We identify and refer suspicious activity through the Financial Crimes Enforcement Network, which law enforcement may access to assist with their investigations. However, on a local level, we recognize that law enforcement has limited resources, and many cases largely go unprosecuted. We would welcome the opportunity to work with our nation's leaders to help prevent fraud and scams, including a more formalized public-private partnership between financial institutions and local law enforcement to help them investigate and prosecute these crimes and bring justice for victims.

Below is the information you requested:

1. *Do you agree with EWS's distinction between fraud and scams for purposes of Regulation E under EFTA?*

   Regulation E does not define "fraud" or "scams". Regulation E states that consumers may be entitled to reimbursement for timely reported unauthorized transactions, i.e., electronic funds transfers that are initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit. We use this guidance to pay out consumer claims under Regulation E. We assess each customer claim based on data available to us and information provided by the customer and take these facts into consideration in order to investigate and evaluate consumer claims in accordance with Regulation E's error resolution requirements. Where a transaction is found to be unauthorized, we fully reimburse the customer.

   a. *Does your bank consider transactions where consumers are fraudulently induced into authorizing a transfer to be covered by Regulation E?*

      Where a customer is fraudulently induced into providing account access credentials to a third-party bad actor and the bad actor initiates an EFT using those credentials, consistent with the CFPB's guidance, we treat those transactions as "unauthorized" under Regulation E and fully reimburse the customer for those timely reported transactions.

2. *What are your bank's current policies and procedures for detecting and eliminating fraud and scams that target your account holders on the online platform Zelle, and how has your bank bolstered those policies and procedures in light of "rampant [...] organized crime" on the platform?*

   Helping to protect customers from fraud and scams is a top priority at Chase. We continue to evolve the ways we alert and message customers when we suspect the possibility of fraud or scams. For example, during payment scenarios with elevated risk-situations, we have implemented new and additional controls to protect our customers from bad actors, such as protective transaction limitations and full page interstitials with prominent, overt language and attention-grabbing titles warning the customer of prevalent scam tactics in market and ways to keep themselves safe. We continue to iterate on these alerts, testing new language and content to assist customers in light of rapidly changing scams and fraud.

   In addition to warnings presented to customers while they are transacting, we also use other available channels to warn customers about scams and provide tips so they can better protect themselves. We

have sent emails directly to our Zelle users, posted warnings on our social media accounts, and have introduced scam education pages that a user sees before sending money.

Banks generally lack the context for why a customer is making a payment or how a recipient plans to use the funds at the time the EFT is initiated by the consumer. However, we still want to assist our clients to avoid scams, and are taking aggressive actions.

3. *What are your bank's policies and procedures for determining which consumers receive refunds for (a) transactions that are unauthorized within the meaning of Regulation E (i.e., where a customer does not initiate a transfer) and (b) transactions that involve scams (i.e., where a customer is fraudulently induced to transfer funds) and that may not be clearly treated as unauthorized by Regulation E?*

   Our policies and procedures follow the requirements of Regulation E and regulatory guidance. After timely notice by a consumer of a transaction that may be considered an "error" as defined under Regulation E, we promptly conduct an investigation to determine if an error has occurred. Claims are investigated based on the information customers provide and other relevant data available to us. Once our investigation is complete, we notify our customers of our decision based on the facts. For errors deemed to be unauthorized transactions after investigation, per the Reg E definition and FAQs guidance, we fully reimburse the customer for the transaction.

   a. *Is this determination made through a joint process with EWS?*

      The determination of whether we accept liability for an unauthorized EFT rests solely with Chase based on the error resolution provisions of Regulation E.

   b. *Are there any standardized policies and procedures among all participating institutions in Zelle?*

      Standardized policies and procedures concerning Zelle are provided by the Zelle Network (EWS) and agreed to by banks participating in the Zelle Network through the Zelle Operating Rules. For example, participating banks, including Chase, provide zero liability to consumers for timely reported unauthorized transactions. Zelle participating banks also agree to attempt good faith courtesy reversal of available funds found in the bad actor's account in order to reimburse for transactions reported by a consumer as scam or fraud.

      Additionally, per EWS' Zelle Rules, when bad actors are detected, Zelle's participant institutions, including Chase, report the transaction to the Zelle network for further monitoring and restriction of access. Internally, Chase will refer the bad actor through an internal investigation and relationship closure. We recognize that local law enforcement has limited resources to pursue many cases of scams – especially so-called "small dollar scams," which are still considerable for the victims but largely go unprosecuted and uninvestigated at the local level. We are supportive of governmental efforts to secure more resources and expertise for law enforcement to combat fraud and scams in all their forms.

4. *How many reports of unauthorized electronic fund transfers (i.e., fraud)- as defined by Regulation E - has your bank received from consumers using the Zelle platform for each of the last five full calendar years, and from January 1, 2022, to the present?*

Chase invests significantly in fraud mitigation efforts across the entire bank, including for Zelle. These efforts have had a direct impact for our customers: every year, Chase prevents nearly $320 million in scams or fraudulent transactions on Zelle, and investigates all reported instances of fraud. When we look at competitors across the P2P industry, the trend continues, with Chase Zelle significantly outperforming them. As noted, consistent with recent industry reporting on P2P network fraud and scams, Chase has also observed much higher off-us fraud on most other major networks than on Chase Zelle.

As noted above, Chase identifies and refers suspicious activity through Suspicious Activity Reports (SARs) filed with the Financial Crimes Enforcement Network, through which law enforcement may access to assist with their investigations. However, on the local level, we recognize that law enforcement has limited resources to pursue many cases of scams – especially so-called "small dollar scams," which are still considerable for the victims but largely go unprosecuted and uninvestigated by law enforcement. We are supportive of governmental efforts to secure more resources and modernize technology that will allow for law enforcement to combat scams in all their forms in more real-time.

From 2017 to August 2022, we have handled ~335K unauthorized fraud claims covered by Reg E and provided refunds to customers in the amount of ~$150mm. This represents ~0.027% of total dollar volume of transactions processed during that period. For year-to-date 2022, this includes ~62K unauthorized fraud claims covered by Reg E and ~$12mm in refunds to customers, representing ~0.009% of dollar volume of transactions.

The number of cases where your bank referred fraud to law enforcement or to federal or state bank regulators.

In the last 5 full calendar years, we have submitted to the government 6,666 referrals that reference "Zelle" and "fraud, scam, scheme". For 2022 YTD June, we have submitted 2,910 referrals.

5. *How many reports of transactions initiated by a consumer that were induced through deception (i.e., scams) has your bank received from consumers using the Zelle platform for each of the last five full calendar years, and from January I, 2022, to the present?*

While scams are infrequent – for Chase Zelle they represent ~0.039% of transactions over the past year – we take them very seriously and have been working cross functionally to better protect our customers from the risk posed by bad actors. We consistently make improvements to our Zelle experience, in the user interface with overt interstitials and warnings, in our risk rules through pilots and feedback loops, via operations with procedural updates and scripting, and with our marketing and public relations partners via direct customer outreach campaigns and utilization of our social channels - all with the goal of better protecting, informing, and educating our customers on the dangers of fraud and scams.

Outside of the internal work we deliver to protect customers from scams, we also work closely with the Zelle Network in trying to ensure bad actors are not able to propagate scams across the platform. We report all instances of fraud and scams to the network, no later than one business day after receiving a report, and work to identify and restrict customers from using the service when we and / or the network have intelligence suggesting they are bad actors. Customer protection is a very high priority for Chase Zelle and we work with industry, relevant networks, media, and law enforcement to protect our customers from scams and bad actors.

Since September 2021, when we increased the granularity of our tracking of non Reg E disputes including scams, we have processed ~131K reported cases of scams with $71mm in value, which represent ~0.039% of total number of transactions. As described above, we are voluntarily refunding customers for "me-to-me" token-registration scams and are cooperating with law enforcement to recover funds where possible.

The number of these scams cases where your bank referred the incident to law enforcement or to federal or state bank regulators.

In the last 5 full calendar years, we have submitted to the government 6,666 referrals that reference "Zelle" and "fraud, scam, scheme". For 2022 YTD June, we have submitted 2,910 referrals.

Respectfully,

Michelle Mesack
Head of US Government Relations
JPMorgan Chase & Co.