Senate Permanent Subcommittee on Investigations
Written Statement of Melissa Feldsher
Managing Director, Head of Commerce Enablement
JPMorganChase
July 23, 2024

Chairman Blumenthal, Ranking Member Johnson, and Members of the Subcommittee, my name is Melissa Feldsher, and I am the Head of Commerce Enablement at JPMorganChase where I have responsibility for our consumer payments business, inclusive of Zelle. Thank you for the opportunity to appear before you today to discuss the critically important topic of criminal fraud and scams.

The digitization of cash has been an undeniably positive development. Digital money is more secure than paper currency and more convenient for consumers. Person-to-person payment platforms have made it easier and safer to send money to family, friends, and others you trust at no additional cost. It is a faster, more convenient, and **more secure alternative to cash and checks** – and meaningfully safer than sending someone cash, checks, or gift cards through the mail. When regulated banks are behind these payments – such as with Zelle – it is safer, cheaper, and better for everyone, and funds are FDIC-insured.

Banks created Zelle in response to the growing demand for a way to securely send money to others they know and trust, in real time, directly from their own bank account. Today, our customers tell us – through surveys and through their increased usage – that they love Chase Zelle for its convenience, speed and seamless integration into Chase.com and Chase Mobile – at no additional cost. Chase Zelle is more than a benefit – it's an expectation of today's banking customers who want this service through their banks.

Fraud and scams have been a persistent blight on society since the earliest days of commerce and have been a consistent public and governmental concern in this country for a very long time. These deceptive practices have evolved over time, but their core intent to exploit and deceive remains unchanged.

What has changed over time is that **criminals – including foreign actors – have fully embraced modern technology**. They sell products that do not exist on social media marketplaces, perpetrate romance scams on online dating sites, and offer nonexistent jobs with an ask for upfront payment. They spoof legitimate businesses and trusted institutions' phone numbers on caller IDs, pretending, for example, to be utilities, banks, and the government. Recent data breaches at large companies will only serve to exacerbate this problem and fuel criminal activity further. Financial scams using all forms of payment – everything from cash, gift cards, cryptocurrency, wires, checks, and person-to-person payments – are an increasing threat to

"Fraud": Fraud on a bank account involves someone illegally accessing someone else's account and making withdrawals, transfers, or purchases without the account holder's permission.

"Scam": A financial scam is a deceptive scheme or trick used to cheat someone out of their money or other valuable assets. Scammers often use false promises, misleading information, or deceptive activities to manipulate victims into giving up something of value. Scams can take many forms, including counterfeit or non-existent products sold on social media marketplaces, phishing emails, fake websites, spoofed Caller IDs on mobile phones, fake profiles on dating sites, fake jobs on job boards, among others.

Americans' public safety and financial health, with implications for our economy and the U.S. financial system.

America's banks are at the forefront of making it harder for these criminals to perpetrate their crimes, but we as a country – the government, law enforcement, banks, social media companies, telecom companies, and many others – must do more to stop this criminal activity at the root.

Even in this difficult environment, American banks stand out for their increased security measures, implementing advanced technologies and rigorous protocols to protect consumers and combat financial fraud. Each year, JPMorganChase proactively identifies nation-state and cybercriminal threats, stopping more than $14 billion in fraud attempts. And **we leveraged that rich expertise and experience and built these protections into Zelle**, the only person-to-person payment network built by the banks.

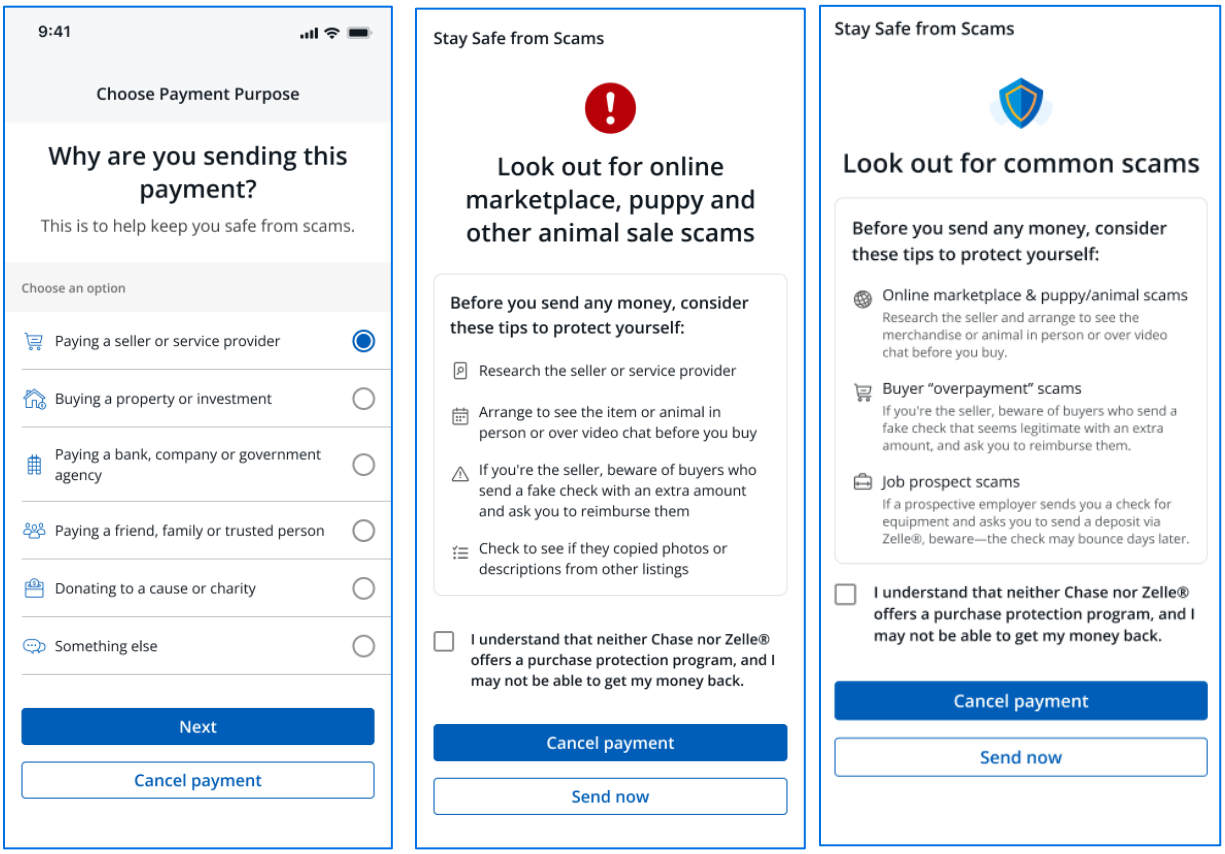
In 2023, the rate of fraud and scam disputes on Chase Zelle was the lowest it had ever been, with only one-half of one-tenth of one percent of transactions (0.05%) ever disputed – a number we have seen further improve in the first half of 2024. We achieved this success through significant expansion of our fraud and scam prevention and detection technical capabilities, as well as a significant expansion of the teams tasked with identifying and combating new fraud and scam patterns on Chase Zelle. Dedicated individuals on these teams focus on a simple truth: **the best way to protect customers from fraud and scams is to prevent criminals from carrying out their schemes in the first place.** We do this in several ways.

- First, **before the customer ever initiates a Zelle transaction**, Chase has already instituted rigorous risk prevention systems which operate outside the immediate view of a Zelle user but significantly limit the ability of criminals to misuse the network. For instance, Chase implements rigorous controls designed to identify and block criminals from accessing the Zelle platform. We do this both through stopping fraudsters from hacking into our customers' accounts, preventing them from accessing Zelle or any other part of the account. Additionally, when we know a bad actor is using Chase Zelle, we block them from Chase Zelle, report it to EWS, and close their bank account.

  We also give our customers critical information that helps them avoid being scammed. We share information with customers about common fraud and scams on social media platforms and the other ways criminals may attempt to trick them into sending their money. Outside of the actual payment experience, we significantly invest in education and scam awareness campaigns. We participate in the American Bankers Association's "Banks Never Ask That" (www.BanksNeverAskThat.com) campaign designed to educate consumers about common tactics used by scammers and to help them recognize and avoid phishing and other types of fraud to help customers avoid falling victim to bank impersonation scams. Understanding many of our older customers may not be as active online, we reached 36 million older customers with direct mail in 2023 and distributed flyers identifying potential scams across all our branches. We have also worked with groups like AARP to develop targeted education programs for its members on the topic.

- Second, **when a customer attempts to initiate a transfer**, Chase institutes rigorous and interactive safeguards which alert customers on how to safely use Zelle as they are attempting to send payments. For instance, we display targeted in-app and web-based warning screens to help prevent scam transfers. For example, because we know that, on Chase Zelle, ***nearly 60% of***

scams originate on social media, we have built in warning screens for customers we believe may be attempting to use Zelle to purchase something on a social marketplace. We give notice that there is no purchase protection on Zelle and that once funds are sent, the customer is unlikely to get them back – just like paying someone cash. These warning screens create friction in the payment process, requiring customers to affirmatively indicate they would like to continue with a payment before it can be processed. This allows our customers to pause and reconsider their transaction.



- Third, **after a customer has initiated a transfer**, Chase channels that Zelle payment into a risk algorithm that gauges the risk of the payment based on an array of factors, and, if necessary, delays or stops the payment altogether. Each month, hundreds of thousands of Zelle payments also undergo manual review by a dedicated team tasked with assessing these payments and, if concerns remain, contacting the customer to confirm the intent. If Chase and our customer are not able to connect, the payment is cancelled.

These efforts have proven successful. Because of this multipronged effort, Chase is able to prevent millions of dollars in fraud and scams. Over the last twelve months, we estimate that our safeguards **prevented Chase customers from exposing nearly $1.1 billion** to possible fraud and scams. We saw **fraud and scam claims plummet in 2023 – each down 14% year over year** – even while total transactions on Chase Zelle were up over 20%.

We all have a vested interest in getting the number of scams perpetrated through the use of Zelle and other forms of payment to "zero." However, we must acknowledge that, despite extraordinary

resources and focus, **banks alone cannot stop financial crimes** that are conceived of and largely executed beyond the boundaries of Zelle. The **heartbreaking losses victims experience at the hands of criminals often go uninvestigated and unprosecuted by law enforcement.** This is particularly true among local law enforcement agencies that often lack the resources to thoroughly investigate, arrest perpetrators, and prosecute these so-called "low dollar" crimes, leaving the victims without justice.

These issues are complex and global. The only way to make real progress against the increasingly sophisticated criminals is through an aggressive and coordinated national response. At JPMorganChase, we applaud and support the countless efforts across industries and government to find solutions to all levels of fraud and scams. We must unify these efforts and **bring the full force of our country – government, law enforcement, banks and nonbank financial institutions, retailers, social media platforms, technology companies, telecommunications companies, and nonprofit organizations – to develop real solutions and ensure we are stopping these crimes at the source**. At JPMorganChase, we have begun such conversations with government, law enforcement, and cross-industry representatives and look forward to working together to stop these crimes.

In closing, I want to thank the Committee for the invitation to speak here today on the important topic of preventing fraud and scams. I look forward to your questions.

###