Fraud, Scams, and the Case for Accountability in Third-Party Payment Platforms

Doug Wheeler

How are you paying for lunch with friends, a haircut, or even the landscaper or plumber to manage household necessities? In today's digital landscape, consumers have moved away from cash transactions to electronic payment methods such as credit cards and third-party payment platforms like Zelle, Venmo, and Cash App. The convenience of being able to reimburse friends for lunch has advanced to allow for ease of use for consumers, allowing them to send funds with just a few taps on their phones safely and quickly while minimizing the need to carry cash. The transaction speed of these payment platforms has made them popular among consumers. However, as their demand and use has surged, so have incidents

of fraud and scams, prompting discussions about legislation and regulation that threaten the ability of providers to offer these services for free to consumers and threaten to up-end the efficiency of the payment model.

Distinguishing Fraud from Scams

According to Federal Trade Commission data,[1] in 2023 consumers reported losing $210 million to fraudsters on payment apps, an increase of 62% from 2021. It is paramount to differentiate between an incident of fraud and being scammed. Fraud typically involves deception where one party unlawfully gains something of value, often through false representation or unauthorized access. For example, this can include common cases of unauthorized persons opening accounts or credit cards under someone else's name. In contrast, being scammed often entails victims willingly engaging in a transaction they believe is legitimate, but being misled about the nature of the deal.

Con artists have evolved to become very effective at posing as legitimate businesses offering a variety of products and services. Phishing scams involve bad actors impersonating legitimate companies or banks to obtain personal information, sometimes through emails warning the reader that their account passwords have been compromised, and other times by convincing consumers to share credentials to verify fictitious transactions. These fake marketplace transactions commonly utilize several factors: One is asking a customer to verify their account by providing their social security number. (A bank will never call to request SSNs as the bank already has that customer information on file when they opened a bank account or credit card). Another is to ask customers to move their funds into a "temporary" or new account to ensure the customer has access to their funds.

Imposter scams may also involve posing as family members or friends in distress and in urgent need of funds, a very common tactic that puts elderly family members at risk of falling for payment scams.

It is also important to note that victims of scams are often prompted to take several built-in "protection" steps[2] to confirm the transaction, such as communicating with the seller or verifying their identity, prior to transferring funds — which only complicates the narrative around who is ultimately responsible in scam cases – the victim or the scammer. Scammers have exploited protections consumers have come to trust, such as two-factor authentication, user-education resources and tips, and fraud monitoring that flags suspicious or unusual transactions and purchasing patterns. So, while platforms like Zelle facilitate these user-generated transactions and protections, unwary users can be vulnerable if they fail to recognize the warning signs that it is a scammer using these "protections" – and they are not being offered by a legitimate platform. It is important for consumers to fully understand the relationship they have with the recipient of the funds.

Let us not forget that fraud and scams have always existed and will continue to exist, and that the source of these problems lies with the criminals perpetrating these scams. Stopping them requires increased law enforcement resources, increased

penalties for when they are caught, improved consumer education, and stronger identification protections to prevent criminals from spoofing users' identities.

Government Efforts for Accountability

In response to the rise in incidents of fraud and scams, government agencies are increasingly looking at how to hold third-party payment platforms more accountable. Initiatives include potential regulations that would require these companies to enhance security measures and fully reimburse consumers for *all* suspected scam transactions.

While regulations may seem like a necessary response, they raise important questions about the balance between consumer protection and the operational viability of these platforms. Stricter regulations could lead to increased compliance costs for companies, which may ultimately be passed on to users as higher transaction fees. This could deter individuals from using these platforms, potentially pushing them back toward less convenient, potentially less secure, and slower methods of payment.

Education Over Regulation

Rather than leaning heavily on regulation, a more effective approach might emphasize more consumer education.[3] Users need to understand the nuances of digital transactions and the potential risks involved. Enhanced educational initiatives could help users identify the red flags associated with scams and make informed decisions *before* sending money.

For instance, platforms like Zelle implemented pop-ups asking consumers to pause and verify the recipient of their funds is recognized before a consumer transfers funds to a new user, highlighting common scams and safe practices. Regular updates and tips would also keep users informed about new and emerging threats. By fostering a culture of awareness, the platforms can continue to empower users to protect themselves more effectively, potentially reducing the number of scam victims without the need for costly and cumbersome regulations.

Consequences of Increased Regulation

The potential consequences of increased government regulation extend beyond higher costs. Stricter rules might also suppress innovation, making it harder for companies to adapt to changing market demands or to integrate new technologies that enhance user experience and security. Furthermore, overly stringent regulations could lead to reduced competition, as smaller players may struggle to comply, ultimately limiting consumer choice.

Ironically, the very essence of third-party payment platforms is their ease of use and immediacy. Adding layers of regulatory compliance could complicate the user experience, resulting in platforms that are less intuitive and user-friendly. Additional regulation may cause these platforms to implement fees for the service to cover the cost of scams while scams unintendingly rise. Picture this: if a scammer knows the initiator of the funds transfer will be reimbursed for complaining of a scam, and the recipient of the scam receives the money (leaving both

sides of the scam fully reimbursed) regulation may incentivize scammers to increase their hustle.

In conclusion, as third-party payment platforms like Zelle and Venmo continue to grow in popularity, the conversation around fraud, scams, and accountability will

undoubtedly intensify. Predictably, the track record of government regulation in innovation and free markets suggests that oversight often leads to more harm than good. With agencies frequently lagging years behind industry trends, their "expert" input is often outdated before it even hits the paper. Instead of fostering a thriving ecosystem of diverse payment options, regulation typically leads to a homogenized market, where innovation is sacrificed at the altar of red tape. So, perhaps it's best to let the market breathe and evolve without the heavy hand of government interference.

While government regulation may play a role, prioritizing consumer education could prove to be a more effective and sustainable solution. By continuing to empower users with knowledge and resources, these platforms can continue offering their valuable services while minimizing the risks associated with fraudulent digital transactions.

Doug Wheeler serves as the Director of the George Gibbs Center for Economic Prosperity at The James Madison Institute.

ENDNOTES

1 Tableau Public - Fraud Reports - By Federal Trade Commission: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts

2 Zelle - How to use Zelle® safely: https://www.zellepay.com/safety-education/use-zelle-safely

3 Zelle - Understanding Scams: https://www.zellepay.com/safety-education/understanding-scams