Consumer Cost Liability for Fraud on Digital Payment Networks

*Contributed by **Kamali P. Willett** & **Andrew M. Parks**, Skadden, Arps, Slate, Meagher & Flom LLP*

November 2023

Who covers your losses if a fraudster gains access to your digital wallet and transfers money to an account you do not recognize? While federal law applicable to credit and debit card transactions is instructive, the answer depends on a number of factors.

With the growing popularity of digital payment networks, this article examines consumers' potential liability for covering the cost of fraud carried out on these networks, including whether and when financial institutions are required to reimburse their customers who have been defrauded.

Increased Prevalence of Digital Payment Networks

With the growing popularity of digital payments, concerns over fraud carried out on digital payment networks have been increasing. As a result, banks have come under increased scrutiny for how they have responded to customers who have fallen victim to fraud using these services.

In an October 2022 report, Senator Elizabeth Warren criticized banks for not reimbursing customers who had been fraudulently induced into making payments on Zelle, or who contest unauthorized Zelle payments. The **report** asserted that there had been "significant increases in the number of fraud and scam claims made by customers over the last two years," and that banks refunded "only 10%" of Zelle scam claims.

On November 13, 2023, media reports began to surface that banks have begun refunding victims of scams carried out on Zelle. Nevertheless, as explained below, existing law may not require banks or other financial institutions to refund their customers.

Existing Law for Credit & Debit Card Fraud

Imagine a thief steals your credit card and uses it to go on a shopping spree. Under the Truth in Lending Act of 1968 and Regulation Z, you could be liable for up to $50, as TILA and Reg Z limit a credit cardholder's liability to a maximum of $50 for the unauthorized use of their credit card.

If the thief had stolen your debit card instead, the law would provide more limited protection. Although the Electronic Fund Transfer Act and Regulation E protect consumers from "unauthorized electronic fund transfers," such as those involving debit cards, the EFTA and Reg E set a three-tier liability structure that provides a consumer with more protection the faster the consumer notifies their financial institution of an unauthorized transfer.

Legal Application to Modern Transactions

The application of TILA, Reg Z, EFTA, and Reg E to digital payment networks turns on several factors, including: the nature of the electronic payment network; the source of funds; the timeliness of reporting fraudulent transactions; the type of fraud at issue; and user agreements that may further limit a customer's liability.

Nature of Digital Payment Network: Pass-through vs. Staged Wallets

Consumers generally access digital payment networks through digital wallets, and not all digital wallets are equal. Some function as "pass-through" wallets, while others function as "staged" wallets. In a pass-through wallet, the digital payment network is merely a proxy for the underlying source of funds, and the wallet itself does not maintain its own balance. Zelle is an example of a pass-through wallet.

Conversely, staged wallets keep a balance, and the funding and payment stages are two distinct steps. The funding comes from underlying source of funds the customer selects that are added to the wallet, and payment entails transferring funds from the staged wallet to the merchant or recipient. PayPal and Cash App are examples of staged wallets.

Pass-through Wallets. For pass through wallets, the customer's liability—and the financial institution's potential responsibility to reimburse—depend on the source of the funds, such as a bank account, debit card, or credit card.

If the transaction is funded by a credit card, it appears that TILA and Reg Z would apply given TILA's broad definition of credit card as "any card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit." See 15 U.S.C. § 1602(l); 12 C.F.R. § 1005.12(a), Comment 1 explaining that Reg Z applies for pass-through wallets that permit direct extensions of credit that do not involve a wallet's asset account. Indeed, the Fourth Circuit has explained that the "core element of a 'credit card' is the account number, not the piece of plastic." *United States v. Bice-Bey*, **701 F.2d 1086**, **1092** (4th Cir. 1983).

If the transaction is funded by a bank account or debit card, it appears that EFTA and Reg E would apply as such a transaction would fall within the definition of an electronic fund transfer, which is "any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account." This can include transfers via an "access device," which is a card, code, or other means of access to a consumer's account that may be used by the consumer to initiate electronic fund transfers.

Staged Wallets. EFTA and Reg E generally apply to staged wallets, as staged wallets count as "financial institutions" subject to Reg E's consumer limited liability requirements because they hold consumer funds in "accounts." An "account" includes a "prepaid account" such as a staged wallet that is capable of being loaded with funds. The Court of Appeals for the D.C. Circuit recently explained that, because "PayPal's digital wallets allow users to store funds for later use," it was subject to Reg E requirements involving prepaid accounts. See *PayPal, Inc. v. Consumer Fin. Protection Bureau*, **58 F.4th 1273**, **1277** (D.C. Cir. 2023).

For transactions involving staged wallets subject to Reg E, a consumer could seek reimbursement—or to avoid liability—from either the digital payment network itself or the bank, depending on the scenario. Because staged wallet transactions consist of both a funding step and a payment step, unauthorized transactions involving staged wallets could arguably constitute two unauthorized transfers—one from a bank account to the digital wallet, and one from the digital wallet to the fraudster, for instance.

Timeliness of Reporting

A financial institution's responsibility to reimburse consumers also depends on how quickly the consumer notifies the financial institution of an unauthorized transaction.

For an unauthorized credit transaction subject to TILA/Reg Z, the consumer is liable for a maximum of $50, unless they notify the card issuer that their account has been compromised before any loss occurs; in which case, the consumer has no liability.

For an unauthorized electronic fund transfer subject to EFTA/Reg E, the consumer is liable for up to $50 if they notify the financial institution within two days of the unauthorized transaction; up to $500 if they take more than two days to notify the financial institution; or potentially the entire amount if the unauthorized transaction appears on a period statement—such as a monthly statement from your bank—and the consumer fails to notify their bank within 60 days of receiving that statement.

Type of Fraud: Scams vs. Unauthorized Transactions

Even if the consumer provides timely notice, under TILA, Reg Z, EFTA, and Reg E, a consumer's potential liability—and, consequently, the financial institution's potential obligation to reimburse—depends on whether the fraud was an "unauthorized" transaction or a "scam." An "unauthorized" transaction refers to a transaction that a consumer did not themself authorize and initiate, while a "scam" refers to a transaction authorized and initiated by a consumer but that was induced through fraud or deception. Existing law appears to protect consumers from unauthorized transactions, but not scams.

Recently, the Consumer Financial Protection Bureau **interpreted** the definition of "unauthorized electronic fund transfer" to include transfers resulting from a consumer being fraudulently induced or misled into providing their account details to a fraudster. And CFPB **interpretations** also provide that a consumer's negligence cannot be used as the basis for imposing greater liability on the consumer.

Even so, these protections may apply only when someone other than the consumer initiates the transaction. Although there is little authority that addresses the issue, two recent cases illustrate this point.

In *Green v. Capital One*, N.A., **557 F. Supp. 3**d 441 (S.D.N.Y. 2021), an accountholder alleged that he had encountered errors while attempting to transfer funds from his account using Cash App. He went online and found what appeared to be customer support line, but what turned out to be a fraudster impersonating a Cash App representative. The fraudster misled him into providing his bank account information, and the fraudster transferred more than a thousand dollars from the accountholder's bank account to the accounts of unknown third parties. The court held that the plaintiff stated a claim against the bank for a violation of the EFTA, finding the plaintiff adequately alleged that the disputed transfers initiated by the fraudster were "unauthorized electronic fund transfers" and that his liability should not have exceeded $50.

The court in *Wilkins v. Navy Federal Credit Union*, No. 22-2916 (SDW) (ESK), **2023 BL 15815** (D.N.J. Jan. 18, 2023) reached a different conclusion where the accountholder had been "scammed" and initiated the transfer herself. There, in response to a voicemail from a fraudster purporting to be an agent at her utility company, the accountholder transferred thousands of dollars to the fraudster via Zelle. Soon after, she realized she had been defrauded and reported the fraud to her credit union, but it refused to reimburse her. The accountholder brought a class action alleging that, among other things, her credit union breached its deposit agreement for failing to reimburse accountholders for losses due to fraud-induced transactions. The court dismissed the case because the plaintiff had "not claimed that someone hacked, took control, or otherwise accessed her Zelle account." Instead, the accountholder alleged "that she, in every sense of the word, *authorized* the . . . transaction."

Notwithstanding these cases, it does not appear that any court has addressed whether banks can limit their liability by taking sufficient precautions to prevent unauthorized access, or that accountholders can incur liability by negligently allowing an unauthorized user to access their account.

User Agreements & "Zero Liability Policies"

Finally, in addition to the limitations of consumer liability under federal law, financial institutions, and digital payment networks have often adopted "zero liability policies" within their user agreements that clarify or supplement the foregoing rules. These policies could, for example, impose further obligations on financial institutions to reimburse their customers, but they cannot modify consumers' rights such as to provide them less protection than federal law grants.

Conclusion

Reasonable minds can differ on the proper allocation of risk with regards to digital payment scams. Fraud on digital networks appears to be increasing, and internet scams are becoming more sophisticated. Accordingly, courts, legislatures, and administrative agencies will have to grapple with the extent to which banks should be expected to bear liability for consumers' mistakes.