Scammers not only carefully plot out seductive scams, but also the best means to receive the consumer's money. This article explains consumers' legal remedies and options, which vary depending on the method used for the consumer's payment. While scammers mostly use payment methods that leave people with little immediate recourse, consumers have options in some situations, and complaining quickly and widely may be the most important way of getting help. A simple resource for consumers who have been scammed is **ReportFraud.FTC.gov** [1].

The first two sections of this article summarize four payment methods that virtually announce that the transaction is a scam and others that wave a big red flag. Advocates should be familiar with these methods when helping clients, friends, or family. The article then turns to a discussion of legal rights and advice on getting money back for scammed consumers despite the consumer's payment using those or other payment methods.

The legal discussion below is in some cases a simplification of more complicated rules, which may have exceptions or differences from the general rules described. With the exception of credit cards, all of the payment methods discussed below are discussed in much more detail in **NCLC's *Consumer Banking and Payments Law*** [2]. Credit card payments are discussed in **NCLC's *Truth in Lending*** [3].

Four Payment Methods That Scream "Scam"

A person contacting the consumer by telephone and requesting any of the following four forms of payment is almost certainly a scammer. Some of these payment methods are illegal even for legal telemarketing operations. Practitioners should be familiar with these somewhat exotic payment methods that may be used by scammers:

- *Gift cards*: The scammer convinces the consumers to go to a nearby store (e.g., Walmart, Target, Walgreens, or CVS) to purchase a gift card. The scammer may even be on the phone with the consumer while the card is being purchased. The scammer then directs the consumer to scratch off the security film on the back of the gift card and read out the numbers to the scammer. The scammer can then remotely access and retrieve the gift card's value or, more commonly, the gift card information will, with blazing speed, be sold and resold on a secondary market. The eventual buyer depletes the card of its value soon after the consumer's gift card purchase. Gift cards are examined in more detail at **NCLC's *Consumer Banking and Payments Law* § 7.7** [4].
- *Cash-to-cash money transfers: The consumer is told to bring cash to a money transfer provider (such as a store acting as an agent for Western Union or MoneyGram) that transfers the value of the cash to another location, often overseas, where the scammer can pick up the cash. Federal law prohibits telemarketers from using this type of payment. See 16 C.F.R. § 310.4(a)(10) and defined by 16 C.F.R. § 310.2(f). See also* **NCLC's *Consumer Banking and Payments Law* § 6.6** *[5].*
- *A cash reload mechanism: The consumer pays cash and a small fee to a retailer for a card or other device that can be used to load cash onto a general purpose, reloadable card. These reload devices (such as MoneyPak, Vanilla Reloads, or Reloadit packs) come with an access code or PIN number. When the consumer provides the access code to the scammer, the scammer can then immediately transfer value from the reload device onto the scammer's own prepaid card. Federal law prohibits telemarketers from using this form of transfer. See 16 C.F.R. § 310.4(a)(10) and defined by 16 C.F.R. § 310.2(g). See also* **NCLC's *Consumer Banking and Payments Law* § 7.2.10** *[6].*
- *Express mail of cash: Some scammers ask the consumer to pay in cash, mailed to the scammer by USPS, FedEx, UPS, or similar next day or other speedy services.*

A Red Flag: A Request for The Consumer's Bank Account and Routing Number

Scammers, telemarketers or other callers may ask for the consumer's bank account and routing number in order to debit the bank account. Those account numbers can be used to take money out of the consumer's account in three different ways, two of which are illegal for telemarketers to use. While entities other than scammers, such as creditors and debt collectors, may use some of these methods, particularly electronic transfers, it is far safer and far less likely to be a scam if the caller is willing to take a credit or debit card.

- *Remotely created checks (RCCs)*, sometimes called telechecks: the seller obtains the consumer's bank account and routing number and prints out a check, and, instead of the consumer's signature, includes language such as "authorized by drawer," which can operate as a legal signature if it is authorized. Federal law prohibits telemarketers from using RCCs. *See* 16 C.F.R. § 310.4(a)(9) and defined by 16 C.F.R. § 310.2(cc). For more detail on RCCs, see **NCLC's**

***Consumer Banking and Payments Law* § 3.13** [7].

• *Remotely created payment orders (RCPOs)* are the same as RCCs, but are never generated as a paper document, but instead are directly submitted through the check clearing system as an electronic image. Because they are never in paper form, RCPOs are not "checks" covered by the Uniform Commercial Code (UCC) and are likely instead covered by the federal Electronic Fund Transfers Act (EFTA). However, RCCs and RCPOs are indistinguishable to the consumer's bank, as paper checks are also typically processed electronically as an image, and banks will process RCPOs as checks. The same federal law prohibits telemarketers from using both RCCs and RCPOs. For more detail on RCPOs, see **NCLC's *Consumer Banking and Payments Law* § 3.13** [7].

• *Electronic fund transfer through the ACH system.* A bank account and routing number can also be used to process an electronic fund transfer (EFT) from the consumer's bank account. The ACH system is the primary electronic system that is used both for direct deposits to consumer accounts and for preauthorized debits from accounts (unless a debit card number is used). ACH payments are legal for telemarketers, and the ACH system has controls against fraud (albeit imperfect) that the check system lacks. For more on EFTs and the ACH system, see **NCLC's *Consumer Banking and Payments Law* §§ 5.1.6.3** [8], **5.3** [9], **5.5.2.2** [10].

The Cardinal Rule: Complain Everywhere, *ASAP*, with As Much Documentation As Possible

Most payment methods used by scammers cannot be reversed (but some can be). While the scammer is legally liable to the consumer, the scammer is usually long gone or is bankrupt when found. Finding a scammer, bringing a lawsuit, and recovering a judgment are generally not practical for an individual scammed consumer. With a few exceptions, described *infra*, a consumer's attempt to stop payment or reverse the payment often is too late or not possible.

Instead, a consumer's best hope may be to file a complaint in as many places as possible, including with the bank or company involved with the payment system and with government authorities. The payment provider may be able to provide help, and an eventual government enforcement action (against the scammer or even against a complicit payment provider or other facilitator) could result in an eventual recovery for victims.

Speed is of the essence. The consumer's chance of recovering money is stronger if the consumer complains quickly, both to payment providers and to law enforcement such as the police and the FBI's Internet Crime Complaint Center (IC3) at **ic3.gov** [11]. It is also important to include as much documentation as possible as to the method of payment, but do not wait for that documentation before filing a complaint.

ReportFraud.FTC.gov [1] is a new, one-stop website for any form of scam and method of payment. The website takes the necessary information from the consumer, advises as to the next steps depending on the nature of the scam and the consumer's payment, and sends the information along to the appropriate law enforcement agencies, including more than 3000 law enforcers. For legal aid and other consumer organizations looking for a data driven way to track fraud reports that the organization files on behalf of consumers, contact mvaca@ftc.gov to get a dedicated link to ReportFraud.FTC.gov.

In addition to **ReportFraud.FTC.gov** [1], for each payment method, consumers should consider filing complaints directly with:

- The bank and any other payment provider or store;
- The police;
- The FBI's Internet Crime Complaint Center (IC3) at **ic3.gov** [11];
- The Consumer Financial Protection Bureau (CFPB) at **https://www.consumerfinance.gov/complaint/** [12];
- The state attorney general.

A recovery for the consumer can come from surprising places. Even cash can sometimes be recovered from the mail. Gift card companies, money transmitters, the FBI, the FTC, the US Postal Inspection Service, and others are looking out for scammers and may have methods to block the consumer's payment to the scammer or otherwise assist the consumer in recovering the consumer's payment. But this may not benefit a scammed consumer unless the consumer files a complaint with the appropriate entity.

For example, Apple and other gift card providers may be able to identify attempts to take value off gift cards coming from overseas internet sites or other suspicious locations. The gift card provider can then block use of the consumer's gift card based on its own anti-fraud processes. But the gift card purchase may not indicate for the gift card provider the identity of the

defrauded consumer. Filing a complaint with Apple, Google, Amazon or other gift card providers, along with a receipt and identification of the gift card, may allow the company to refund the gift card amount to the consumer.

In another example, in bank-to-bank transfers, the FBI's Recovery Asset Team (RAT) may recover a complaining consumer's money by contacting both banks and the scammer. The RAT team focuses on larger losses.

The FTC and Department of Justice have also recovered hundreds of millions of dollars from intermediaries such as Western Union, payment processors, voice over internet providers, and others that facilitate scams. The CFPB has a victim recovery fund that can be used to compensate consumers even when the scammer is in bankruptcy. The best way for a consumer to be included in the list of restitution recipients in actions brought by these agencies, if the scammer's or payment providers records do not identify the victims, is where the consumer has contemporaneously filed a complaint and identified themselves as a victim. Filing a complaint is also important because an accumulation of complaints can lead to law enforcement actions against either the scammer or complicit intermediaries that may lead to restitution.

The discussion below contains more specific advice on where to complain depending on the payment method used.

Consumer Payments by Mail—Cash, Money Orders, and Similar Items

If a consumer sends cash, money orders, or similar items to a scammer via the U.S. Mail, the consumer should immediately call the U.S. Postal Inspection Service at 877-876-2455 to report the fraud. Scammers often require next day or other special delivery that will involve a tracking number—providing this can be of great help to the Inspection Service. The Inspection Service has a number of effective ways to help consumers in mail fraud cases—but time is of the essence.

Contacting the Inspection Service is always the best approach. Consumers with the tracking information can also try to have the Post Office intercept the consumer's mailed package, as described **here** [13]. If the consumer used UPS, FedEx, or another delivery service, contact that service instead.

Laws Applicable to Payments Directly Out of the Consumer's Bank, Prepaid, or P2P Account

Today there are varied ways for a scammer to be paid directly out of the consumer's bank account without the use of a paper check signed by the consumer. The consumer's legal rights will vary by the method used.

The EFTA and **Regulation E** [14] cover a wide variety of electronic fund transfers (EFTs), including those made through the ACH system, debit or prepaid card payments, consumer initiated "push payments" like Zelle, PayPal, or Venmo, and wire transfers made through a bank (but not through Western Union or other money service businesses). *See* **NCLC's *Consumer Banking and Payments Law* Chapter 5** [15].

Payments from prepaid card accounts are covered by most of the same rules that govern bank accounts. Many person-to-person (P2P) systems, such as Venmo and PayPal, are technically prepaid accounts. For more on prepaid accounts, see **NCLC's *Consumer Banking and Payments Law* Chapter 7** [16].

As discussed above, RCCs are covered by state UCC laws. The coverage of RCPOs has not been resolved, and technically they are likely EFTs, but in practice the are indistinguishable from RCCs and banks will treat them like checks.

Check or Deposit Scams

Many payment scams begin with a check payment *to* the consumer. There are many **varieties of these scams** [17], including mystery shopping, personal assistants, car wrap decals, sweepstakes prizes, and overpayments. Whatever the supposed reason for the check payment to the consumer, the consumer is given a check to deposit and is told that they can keep a portion of the check and then must send the remainder to the scammer, often by gift card, money order, or wire transfer.

The consumer deposits the check, sees that the money in their account, and then withdraws or transfers funds to pay the scammer. But then the check deposit is reversed after the check turns out to be a fake or drawn on a closed account. The consumer is fooled because having the funds "available" in the account does not mean that the check has cleared. The

Expedited Funds Availability Act requires banks to make a portion of deposited checks "available" quickly, usually within two days. *See* **NCLC's *Consumer Banking and Payments Law* § 4.5** [18]. In practice, banks often make the entire check (not just a portion) available before it has fully cleared. But fake checks can take weeks to be untangled and have not "cleared" during that period.

U.C.C. § 4-214 allows the bank to chargeback the consumer's account if the check fails to clear. *See* **NCLC's *Consumer Banking and Payments Law* § 4.8.3** [19]. Consumers may attempt to assert a common law claim or defense against the bank if the bank's negligence led the consumer into believing that the check had cleared. But merely stating that the funds are available is not the same as misrepresenting that a check has fully cleared. Consumers are more likely to prevail in these situations when the claim is asserted as a defense to a bank's attempt to collect a negative balance against the consumer than when the consumer seeks a refund from the bank. Check scams are discussed in **NCLC's *Consumer Banking and Payments Law* § 4.8.6** [20].

The same type of scam can also happen with an electronic deposit that is reversed, such as when the payment is sent from the account of another victimized, hacked consumer. In either situation, the consumer's legal rights regarding the separate payment to the scammer are governed by the type of payment at issue.

Where to Complain About Payments from the Consumer's Bank Account

When payment to a scammer comes from a bank account, whatever the method of payment to the scammer, consumers should immediately contact their bank to see if the bank can stop the transaction or otherwise return the money to the consumer. If the payment was initiated from PayPal, the Cash App, or another payment system, the consumer should complain there too.

Even if the payment cannot be stopped and there is no legal right to reverse it, the consumer should insist that the bank take a complaint, investigate, and forward the complaint to the bank or check casher on the receiving end. While the money may not have gone directly into an account owned by the scammer (it could go into an account opened with a stolen identity or to a "**money mule** [21]" account owned by another defrauded consumer), the receiving institution should be told that the account is being used for fraudulent purposes. That institution may have ways of freezing or recovering funds.

In addition to complaining to the bank, especially if the loss is large, the consumer should *immediately* file a complaint with the FBI's Internet Crime Complaint Center (IC3) at **ic3.gov** [11]. The center will refer the matter to the appropriate agency. If the consumer transferred a large amount of money and provides full financial transaction information, the FBI's Recovery Asset Team (RAT) may be triggered. According to its 2019 annual report, in more than 1300 instances where RAT was triggered, the team had a recovery rate of nearly 80%. The consumer should also submit a complaint to the CFPB at **https://www.consumerfinance.gov/complaint/** [12].

Rights to Stop or Reverse Payments from Bank Accounts

State or federal law gives consumers the right to stop payment of checks (including RCCs and, in practice, RCPOs) and preauthorized, recurring EFTs (including recurring ACH payments and recurring debit or prepaid card payments). NACHA rules (the private organization that oversees the ACH system) also provide a stop payment right for some one-time preauthorized ACH payments. But in practice, when a consumer has been scammed, it will usually be too late to stop the payment. And neither the EFTA nor NACHA rules provide any right to stop or reverse consumer-initiated electronic payments, such as those made through Zelle, Venmo, PayPal, or the Cash App.

Consumers may have better luck disputing a payment after the fact. State UCC laws give consumers the right to dispute unauthorized "signatures" on checks, including RCCs. *See* **NCLC's *Consumer Banking and Payments Law* § 3.7.2.4** [22].

The EFTA provides dispute rights for unauthorized EFTs. All EFTs, including those made through Zelle or Venmo, may be disputed as unauthorized if the payment was not initiated by the consumer. But the EFTA defines an unauthorized transfer as one "initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit." 15 U.S.C. § 1693a(12); 12 C.F.R. § 1005.2(m). For more on the EFTA and unauthorized transfers, see **NCLC's *Consumer Banking and Payments Law* §§ 5.3** [9], **5.5** [23], **5.6** [24].

Thus, if the consumer initiated a Zelle, Venmo, or other payment (such as by making a debit card purchase), the EFTA does not allow the consumer to dispute the charge as unauthorized charge, even if the payment was induced by fraud. But in some cases, depending on the circumstances, the private rules of the payment network (PayPal, Visa, MasterCard) or the website

where an item was purchased (eBay, Amazon) may allow the consumer to dispute the charge if they did not get what they paid for. (Debit cards do not have the same chargeback rights as credit cards, discussed below.)

Some scam payments are initiated by the scammer, such as where the scammer initiates an ACH electronic payment or a debit card payment after obtaining the consumer's bank account or debit card number on the phone. Those payments are potentially disputable if they otherwise meet the EFTA's definition of unauthorized transfer and the consumer's purported authorization was procured through fraud.

While the EFTA does not generally specify the requirements for authorizing a charge, it does for preauthorized EFTs (PEFTs), which are EFTs sent to the payee that recur at regular intervals. If a charge is not properly authorized, then it should be disputable as unauthorized under EFTA rules. PEFTs must be authorized by a writing signed or similarly authenticated by the consumer that is readily identifiable as an authorization with clear and readily understandable terms. 12 C.F.R. § 1005.10(b); Reg. E, Official Interpretations § 1005.10(b)-6. (In some cases, the writing requirement may be satisfied electronically or even on the phone, such as by typing a code.) PEFTs are discussed at **NCLC's *Consumer Banking and Payments Law* § 5.9** [25]. NACHA rules have similar authorization requirements that cover one-time EFTs through the ACH system. *See* ***id.* § 5.3** *[9].*

Whatever the merits of the consumer's unauthorized use claim, under the EFTA, the financial institution (including a bank, prepaid company, or P2P provider) must investigate the claim. It generally is only required to examine its own records, but the investigation must be reasonable. If the financial institution cannot complete the investigation within 10 business days, it must provisionally credit the consumer's account in the amount of the alleged error and then may take up to 45 days to finish the investigation. 12 C.F.R. § 1005.11(c). There are some exceptions to these deadlines.

The financial institution must report its findings to the consumer within three days of completing its investigation. If it determines that the charge was unauthorized, it must reverse the charge within one business day of that determination. 12 C.F.R. § 1005.11(c)(1).

If the financial institution finds no error, or a different error than the consumer alleged, it must provide a written explanation of its findings and note the consumer's right to request the documents on which the institution relied. Upon request, the institution must promptly provide copies of the documents. 12 C.F.R. § 1005.11(d)(1). For more on the EFTA's error resolution procedures, see **NCLC's *Consumer Banking and Payments Law* § 5.6** [24].

In any action under the EFTA involving the consumer's liability for an EFT, the burden of proof is on the financial institution to show that the charge was authorized. 15 U.S.C. § 1693g(b).

If the EFT was made through the ACH system, NACHA rules provide more protection from unauthorized transfers involving telemarketing than does the EFTA. Under NACHA rules, a transfer is authorized only if the scammer has obtained the consumer's written or electronic signed authorization for the transfer. While exceptions to this signature requirement apply where the consumer provides transfer information over the telephone, these exceptions do not apply where a scammer without an existing relationship with the consumer initiates the call (a cold call). NACHA rules thus define as unauthorized an EFT initiated through a cold call without the consumer's signed authorization.

The consumer has 60 days from the sending of the monthly bank account statement containing the charge to dispute it. (If an access device has been lost or stolen, the consumer could be liable for subsequent unauthorized charges if the loss is not reported within two business days.) For more on the EFTA's liability limits, see **NCLC's *Consumer Banking and Payments Law* § 5.5** [23].

The same rules for disputing unauthorized charges, with some slight adjustments to deadlines, generally apply to prepaid cards as to bank accounts. But the EFTA's protections only apply after the consumer has registered the prepaid card in the consumer's name. *See* **NCLC's *Consumer Banking and Payments Law* § 7.2.3.9** [26]. Unregistered prepaid cards are essentially the same as gift cards.

Gift Cards

When the consumer pays a scammer using a gift card or prepaid reload pack, a consumer's best course of action is to contact the gift card issuer and tell it that the consumer is a scam victim. Time is of the essence, and the consumer should provide all receipts. There are no federal protections for payments by gift card other than fee and expiration limits, but the gift card issuer may help voluntarily. In the unlikely event that the card's value has not been depleted, the gift card issuer may be able to block value coming off the card.

In addition, gift card issuers often have anti-fraud processes monitoring for suspicious activity and may block a gift card on their own. But the gift card issuer typically will not know the consumer's identity because it is not linked to the card. By filing a complaint with the gift card issuer, the consumer can alert the issuer about the fraud and learn whether the value of the card was redeemed. If it was not redeemed, it may be possible to obtain a refund. The card issuer may require that the consumer produce the physical gift card, the gift card receipt, and may even require that the consumer file a police report. Contact information for six of the most popular gift cards is as follows:

- Amazon: (888) 280-4331 or click **here** [27].
- eBay: (866) 305-3229, say "representative" at the first prompt, then "gift card" after the next prompt. For more information, click **here** [28].
- Google Play: (855) 466-4438 or report gift card scams **here** [29].
- iTunes: Apple Support at (800) 275-2273 and say "gift card" at the prompt or click **here** [30].
- Steam: report gift card scams online **here** [31].
- MoneyPak (Green Dot): (866) 795-7969 or contact **here** [32].

Wires Not from a Bank Account

Wire transfers not involving banks are virtually the same as sending cash—there are no payment protections against a scammer. Typically, there is no way to reverse the transaction or trace the money. When money is wired, the recipient can pick it up at one of many locations, making it nearly impossible to identify the recipient or track him down.

The best approach is to immediately contact the company that transmitted the wire transfer to file a fraud complaint and ask for the transfer to be reversed: MoneyGram at 800-666-3947 or Western Union at 800-325-6000. These wires in a telemarketing transaction are illegal. *See* 16 C.F.R. § 310.4(a)(10) and defined by 16 C.F.R. § 310.2(f). If the consumer, when initiating the wire transfer, informed the Western Union or MoneyGram agent of the telemarketing nature of the transaction, the wire transmitter company may have liability for the wire violating this federal requirement, even if the wire transmitter's boilerplate language asks the consumer to certify that the transfer does not involve telemarketing. As with other types of payments, the consumer should also file a complaint with **ReportFraud.FTC.gov** [1] and other government authorities.

A Western Union or MoneyGram wire transfer often does not involve a Western Union or MoneyGram office, but instead the consumer goes to a local store that is an agent of the wire transmitter, and the scammer goes to another store that also is a Western Union or MoneyGram agent. Western Union and MoneyGram may be investigating agents linked to scammers and may be willing to reimburse consumers where their agents participated in the fraud.

Money Orders

To stop payment on a money order, contact the company that issued the money order right away. Since the money order will have been mailed to the scammer, also see the discussion, *supra*, regarding mailed payments.

Credit Card Payments

Unlike most other forms of payment, the consumer has a good chance of reversing a credit card payment to a scammer, and the consumer need not act immediately. While most scammers do not take credit cards, credit card rights may be useful when problems may arise for online purchases for goods or services not provided as promised (i.e., fake COVID protection items).

Three independent federal rights protect consumers paying by credit card. As a practical matter, in most cases, the consumer should first contact the seller/scammer. If the scammer is unwilling to reverse the charge, the consumer's initial notice to the card issuer asking for a chargeback will be sufficient to start the process, without asserting one of the three specific federal rights. This initial notice can be done by calling the card issuer or often can be done through a consumer's online account with the card issuer.

The card issuer may provide a form for a written confirmation—otherwise the consumer should confirm in writing the request to cancel the charge. **Click here** [33] for a sample letter from the Federal Trade Commission, but it may not be appropriate in all cases.

Where a claim is meritorious, the consumer is likely to receive the chargeback, but the advocate should be familiar with the federal protections underlying the card issuer's chargeback. Far more detail than the following brief summary on these three federal rights is found in **NCLC's *Truth in Lending* §§ 7.9** [34], **7.10** [35], and **7.11** [36].

The first federal right relates to unauthorized use of the card, defined as "a use of a credit card by a person other than the cardholder who does not have actual, implied, or apparent authority for such use and from which the cardholder receives no benefit." 15 U.S.C. § 1602(p). Unauthorized use protections may not apply where the consumer provides the card number for the specific use, such as in response to the scam offer. But if the scammer or anyone else charges the card for something else, the use is unauthorized. Maximum liability for unauthorized use is $50 and in most cases the consumer will have zero liability, either by operation of law or by the card issuer's policy. *See* **NCLC's *Truth in Lending* § 7.10.4** [37]. There is no written notice requirement or a deadline to make the claim of unauthorized use.

The second federal right relates to billing error resolution. See 15 U.S.C. §§ 1666–1666j. A billing error includes an unauthorized charge, a charge in a higher amount than authorized, or charges for goods or services not delivered, delivered late, or different from that agreed upon. Quality disputes are not billing errors. *See* **NCLC's *Truth in Lending* § 7.9.4** [38]. Federal law requires billing error notices to be submitted in writing within 60 days of the card issuer sending a credit card statement that includes the disputed charge. The consumer's notice to the card issuer should identify the consumer and the account number and state in general terms why the consumer is seeking a chargeback.

The third federal right makes a card issuer subject to all claims the consumer can raise against the scammer. See 15 U.S.C. § 1666i.The consumer should not pay the disputed amount while asserting this federal right. There are three other limitations that typically are not relevant in a scammed transaction: the matter must be over $50, the consumer must have tried to resolve the matter with the scammer (unsuccessfully reaching the scammer should satisfy this requirement), and the transaction must have occurred in the consumer's home state or within 100 miles of the consumer's address (state law will typically find the transaction occurred where the consumer was contacted, not where the call was initiated). *See* **NCLC's *Truth in Lending* § 7.11.2** [39]. This federal right applies to almost any claim the cardholder has against the scammer.

Thanks

Special thanks to Monica Vaca, Associate Director, Division of Consumer Response & Operations, Federal Trade Commission, for responding to our many questions. NCLC is solely responsible for the content of this article, and it does not necessarily reflect the views of Ms. Vaca or the Federal Trade Commission.

Author Name: Lauren Saunders
About Author:
Lauren Saunders is Associate Director at the National Consumer Law Center and manages the Washington, DC office, where she directs NCLC's federal legislative and regulatory work. Lauren is a recognized expert in various areas, including small dollar loans, fintech, prepaid cards, credit cards, bank accounts, and consumer protection regulation. She is the lead author of ***Consumer Banking and Payments Law*** [40], contributes to ***Consumer Credit Regulation*** [41], and has authored several reports and white papers. She previously directed the Federal Rights Project of the National Senior Citizens Law Center; was Deputy Director of Litigation at Bet Tzedek Legal Services; and was an associate at Hall & Phillips. She graduated magna cum laude from Harvard Law School and was an Executive Editor of the Harvard Law Review, and holds a Masters in Public Policy from Harvard's Kennedy School of Government and a B.A., Phi Beta Kappa, from Stanford University.

Source: National Consumer Law Center, [], updated at www.nclc.org/library
Source URL: https://library.nclc.org/getting-money-back-scammed-consumers

Links
[1] https://reportfraud.ftc.gov/#/
[2] https://library.nclc.org/nclc/link/CBP.01
[3] https://library.nclc.org/nclc/link/TIL.01
[4] https://library.nclc.org/nclc/link/CBP.07.07
[5] https://library.nclc.org/nclc/link/CBP.06.06.01
[6] https://library.nclc.org/nclc/link/CBP.07.02.10
[7] https://library.nclc.org/nclc/link/CBP.03.13.01
[8] https://library.nclc.org/nclc/link/CBP.05.01.06.03
[9] https://library.nclc.org/nclc/link/CBP.05.03
[10] https://library.nclc.org/nclc/link/CBP.05.05.02.02
[11] https://www.ic3.gov
[12] https://www.consumerfinance.gov/complaint/
[13] https://faq.usps.com/s/article/USPS-Package-Intercept-The-Basics
[14] https://www.consumerfinance.gov/rules-policy/regulations/1005/
[15] https://library.nclc.org/nclc/link/CBP.05
[16] https://library.nclc.org/nclc/link/CBP.07
[17] https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-fake-check-scams
[18] https://library.nclc.org/nclc/link/CBP.04.05
[19] https://library.nclc.org/nclc/link/CBP.04.08.03
[20] https://library.nclc.org/nclc/link/CBP.04.08.06
[21] https://www.consumer.ftc.gov/blog/2020/03/whats-money-mule-scam
[22] https://library.nclc.org/nclc/link/CBP.03.07.02.04
[23] https://library.nclc.org/nclc/link/CBP.05.05
[24] https://library.nclc.org/nclc/link/CBP.05.06
[25] https://library.nclc.org/nclc/link/CBP.05.09
[26] https://library.nclc.org/nclc/link/CBP.07.02.03.09
[27] https://www.amazon.com/giftcardscams/b?ie=UTF8&node=15435487011

[28] https://www.ebay.com/help/buying/paying-items/ebay-gift-cards?id=4640#section4
[29] https://support.google.com/googleplay/answer/9057338?hl=en&ref_topic=9057343
[30] https://support.apple.com/itunes-gift-card-scams
[31] https://help.steampowered.com/en
[32] https://www.moneypak.com/security
[33] https://www.consumer.ftc.gov/articles/0385-sample-letter-disputing-billing-errors
[34] https://library.nclc.org/nclc/link/TIL.07.09
[35] https://library.nclc.org/nclc/link/TIL.07.10
[36] https://library.nclc.org/nclc/link/TIL.07.11
[37] https://library.nclc.org/nclc/link/TIL.07.10.04
[38] https://library.nclc.org/nclc/link/TIL.07.09.04
[39] https://library.nclc.org/nclc/link/TIL.07.11.02
[40] https://library.nclc.org/cbp
[41] https://library.nclc.org/ccr
[42] https://disqus.com/?ref_noscript