pipl

Four Ways Fraudsters Are Taking Their Tactics to New Levels

A Pandemic Followed by an Epidemic

2020 unleashed more than a disease pandemic—it also precipitated an epidemic of eCommerce fraud. As merchants experienced 25-30% increases in card-not-present (CNP) transactions during the pandemic, fraudsters capitalized. Although "friendly" chargeback and refund fraud was prevalent pre-Covid, fraudsters have elevated these types of fraud to almost an art form. In addition to losses created from cardholders' attempts to refund transactions, organized networks of professional fraudsters are working full time—with legitimate cardholders or cardholder data—to bilk merchants, payment card companies, banks, and consumers of billions of dollars.

CNP fraud losses are projected to total **$7.9 billion** in 2021.

How much are we talking about?

The vast majority of CNP fraud occurs after a transaction. Although risk and fraud analysts work to detect and prevent fraudulent transactions from being fulfilled, that's pretty difficult to accomplish when the fraudster IS the cardholder or when he is using the legitimate cardholder's information. As a result, CNP fraud losses are rising quickly. According to Aite Group, CNP fraud losses are projected to total $7.9 billion in 2021.

For an average business, costs add up quickly:

- Value of the stolen goods
- **Order fulfillment costs**
  Businesses still pay the cost of producing, storing, and packaging orders
- **Shipping costs**
  Carrier and delivery costs cannot be recouped
- **Payment processing fees**
  Service fees charged for the sales transaction cannot be recaptured
- **Chargeback fees**
  Payment processors fine merchants for chargebacks on their accounts
- **Higher processing fees**
  Card processing fees rise if a business exceeds a certain level of chargebacks
- **Loss of card processing abilities**
  Worst case, a merchant's card transaction processing abilities are suspended or revoked
- **Costs of fighting the problem**
  At the end of the day, merchants have to dedicate time, staff, and money to fighting fraud, instead of being able to focus those resources on their core business

Why is it Happening?

Digital payment fraud, such as chargeback fraud, traditionally has been easier to commit against online merchants. Fraud detection solutions and best practices for online merchants haven't kept pace with skyrocketing CNP transactions. However in 2020, brick-and-mortar businesses also have been hit hard as they try to accommodate customers with new contactless, curbside pickup, and delivery services. Neither have regulatory measures kept pace with the ecommerce explosion—patterned after 1970s-era consumers, chargeback regulations have not adapted to the real-time online world.

Consumer expectations have overwhelmed merchants' abilities to keep up. Best case, in a "have-to-have-it-now" world, consumers are unwilling to wait for a refund if they want to return merchandise. Instead, they initiate a chargeback with the bank because they believe it's faster and more efficient. Chargeback process loopholes enable this type of behavior, and most cardholders don't realize that their impatience costs merchants big time. Worst case, consumers intentionally commit fraud to satisfy their need for immediate gratification.

Banks are also overwhelmed by chargebacks. They don't have the resources to investigate every cardholder chargeback, so they simply submit them to the merchant's acquiring bank. As a result, merchants are hit with higher fees, and consumers face no consequences for their actions.

Merchants have the right to challenge chargebacks, but in reality, it's a lengthy, complicated process. As card issuers and banks work hard to be consumer-friendly, the burden of proof lies on the merchant. They must validate the original transaction and produce evidence. In the end, they rarely win, and to add insult to injury, there's not much they can do to prevent the cardholder from doing it again.

1

Chargeback Fraudsters Attack New Channels

Chargeback fraud has been around a long time. The perpetrators often are authorized cardholders who dispute what seem to be legitimate charges to their credit cards. The card might have been used knowingly by the authorized cardholder or unknowingly by a spouse or teen. Using cardholder credentials becomes even easier to do when they're stored on multiple devices used by multiple family members. Until there's a dispute, it's nearly impossible to detect a friendly fraudster in the act.

When there is a dispute, it can be for several reasons. Perhaps the authorized cardholder wants to avoid paying for the goods. Maybe they forgot they made the purchase. Or they don't recognize the transaction because someone else in the household made the purchase. In any case, the customer wants the money returned and does not return the product or services rendered. The most common excuses given for chargebacks are:

- The item or service wasn't delivered
- The item or service wasn't as described—instead it was the wrong color, size, defective, or counterfeit
- It was the merchant's mistake for not canceling a recurring payment when requested

Chargeback fraudsters mined a new channel during the pandemic. Between late February and late March 2020, Adobe Analytics noted that buy-online-pick-up-in-store orders (including curbside) increased 87% year over year—and 80% of consumers plan to continue this habit moving forward. The food and beverage industry has been particularly hard-hit because food is perishable and many of these businesses are small. They don't have fraud prevention programs in place and are not equipped to recoup losses. In addition, chargeback amounts are usually low, so it might be weeks or months before a restaurant or delivery service realizes that they are victims. According to data from fund recovery firm MyChargeBack, there was a 68% increase in month-over-month, dispute-related requests between February and April 2020 for transactions less than $5,000. And unfortunately, analysts believe that up to 83% of friendly fraudsters who get away with it become repeat offenders.

2

Refund Fraud Spawns New Variations

The pandemic with its related unemployment and economic difficulties also motivated people to seek new ways of "saving" money. A rising tide of refund fraud—also known as shipping or cargo loss fraud—is emerging. Refund fraud by a legitimate cardholder is similar to chargeback fraud but with a different motive—they fully intend to use the merchant's refund policies to receive the money back or to receive an additional product.

Because refund fraud occurs without a card chargeback or a traditional payment dispute mediated by a bank or payment processor, it's hard for merchants to detect. When they become aware of growing losses associated with refunds, this type of fraud is still hard to fight. It takes time, resources, and significant effort to determine if refunds are rising because of mistakes in the warehouse or if a bad actor is at work. In 2020, merchants reported a 49% increase in promotional abuse and a refund fraud growth of 51%.

Fraudsters are taking full advantage of many merchants' inability to detect or fight refund fraud. Professional refund fraudsters use social engineering or recruit "mule" cardholder accomplices to help them profit. They provide refund-as-a-service, requesting a fee (often in cryptocurrency) from the cardholder, who in turn makes a large-dollar purchase, receives a refund, and keeps the merchandise. The fee can range from 15-30% of the order value. After the purchase transaction, the fraudster contacts the merchant's customer service personnel. Using knowledge of the cardholder and merchant's refund policies, the fraudster impersonates the cardholder and demands a refund. These professional refunders often post their services on web and social media forums—even outlining guidelines that 'must be followed' and companies that 'guarantee' refunds.

The most common ways that fraudsters execute refund fraud:

Did not arrive (DNA) refund fraud

Fraudsters contact the merchant's customer service team claiming that a package never arrived or was stolen by a porch pirate. They do not dispute the original purchase, but attack the merchant's fulfillment or logistics practices. In many cases, the merchant knows that the package was delivered or the customer signed for it, but is hesitant to create customer friction and so they grant the refund.

Empty box (EB) or partially empty box (PEB) refund fraud

In this scenario, the fraudster claims that the item was stolen during shipping or that a small, expensive item was not in the box with a larger, low-priced item. Again, with little control over logistics, merchants feel forced to make refunds.

Fake tracking ID (FTID) refund fraud

This type of fraud is complex. Here, the bad actor requests a refund for a high-priced item. The business needs the item returned before issuing a refund, so they send a shipping label to the bad actor. Now the fraudster attaches the shipping label to a regular envelope—not a box—that goes back to the merchant's regular mailbox. Typically it looks like junk mail and is tossed out. The fraudster claims they returned the item and needs their money back.

3

Return Fraud & Abuse Costs Retailers Even More

Return fraud occurs when fraudsters take advantage of customer-friendly return policies to profit or get free products. Return abuse is a related type of fraud. In this case, the cardholder buys a product intending to use it once and then returns it. Think high-priced, large-screen TVs purchased before major sporting events.

Return fraud costs businesses a lot. According to the 2019 Appriss Returns in the Retail Industry report, merchandise returns cost U.S. retailers $309 billion—$41 billion from returns of online purchases. Of the total, an estimated $27 billion in losses came from merchandise return fraud.

- **Clothing return fraud**
  Fraudsters wear or use clothing intending to return it later. This is small-time fraud, but even if returned items are lightly used, they can't be resold at full price. The retailer loses the sale on the return and loses more on markdowns.
- **Multichannel return fraud**
  When merchants sell through physical stores and online outlets, they will see this type of fraud. Here, a fraudster buys products with a stolen credit card and then tries to return them for cash refunds.
- **Check or gift card fraud**
  In this case, a fraudster purchases something with a forged check or stolen gift card and returns the item for cash before the check or gift card balance clears.
- **Price manipulation return fraud**
  This occurs when fraudsters try to return stolen goods or manipulate tags or packaging to return something for more than it's worth. They might alter the price tag to increase the item's price and try to return it for cash. Or they might replace a high-priced product with a low-priced one in the package and try to return it.

4

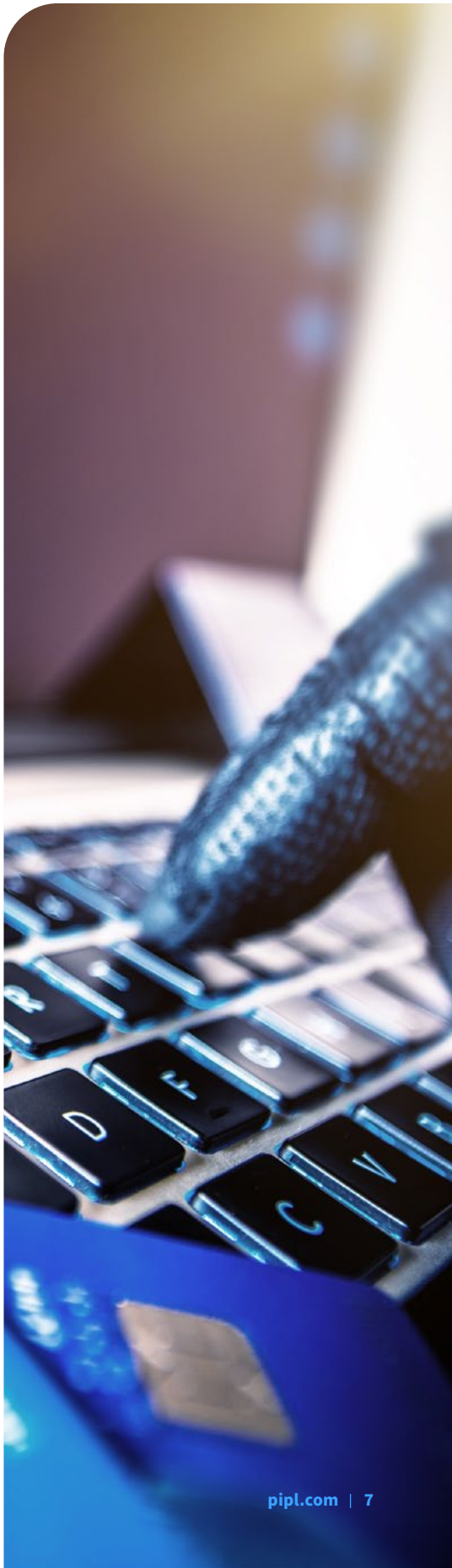
Buy Now Pay Later Fraud Ramps Up

“Pay later” offerings hit headlines in September 2020 as Microsoft and PayPal announced new payment offerings that allow customers to pay for purchases in installments. Buy Now Pay Later (BNPL) schemes offer fraudsters greater convenience too. Fraudsters often use stolen identities or other personal details to set up accounts with payment services. Then they shop. Consumers whose details are stolen and used in this way are unaware that these accounts exist until they receive a bill or collection letter demanding payment, which can be several months later. Fraudsters can do a lot of damage to the consumer, the payment service, and the merchants involved during the time between opening the account and being detected.

Fighting Back

Fraudsters never stop coming up with ways to illegally gain money or products. Fighting multifaceted friendly fraud requires a cohesive strategy with multiple tactics. Critical to fraud prevention and detection is a strong identity verification platform. Pipl provides access to more than 3 billion trusted identity profiles that help fraud analysts and investigators quickly narrow their focus to their targets.

For more information, visit pipl.com.



ABOUT PIPL

Pipl is the world’s leading provider of online identity information. With unmatched global coverage of over 3 billion online identities compiled and cross-referenced from over 25 billion identity records, Pipl is the choice of professionals worldwide.