Visa Direct

Fraud Risk FAQs

1. What is the difference between unauthorized payment fraud and authorized push-payment fraud?

- Unauthorized payment fraud occurs when a fraudster uses your Visa card without your permission to fund a Peer-to-Peer ("P2P") payment to themselves or an associate. They might use stolen Visa card details to fund the payment or hack into your P2P account and use your Visa card registered on the account.
- Authorized push-payment fraud, or scam fraud, occurs when a fraudster convinces a consumer to send funds via a P2P service and there is a scam involved – like paying for a non-existent product or service or sending money to the wrong person. In this scenario, the cardholder initiates or gives permission for the payment from their account to fund the payment.

2. What are some of the primary tactics fraudsters use to scam their victims.

- Social Engineering: Fraudsters and scammers frequently rely on social engineering to trick, or lure victims into authorizing payments. Social engineering is fundamentally a con. It's a trick that relies on psychological manipulation in order to get a victim to reveal confidential information or undertake specific actions (i.e. initiate or authorize a payment).
- Phishing: Criminals and fraudsters frequently rely on e-mail, although they may use other channels, including, SMS and text messages, social media, messaging apps, and phone calls to induce individuals to reveal personal information, including, but not limited to passwords, PINs, credit card numbers or other sensitive information.

3. What is Visa's Zero Liability Policy and does it cover unauthorized fraud?

- Visa's Zero Liability Policy is our guarantee that you won't be held responsible for unauthorized charges made with your account or account information. You're protected if your Visa credit1 or debit card is lost, stolen or fraudulently used, online or offline.

  In instances of unauthorized fraud, a fraudster uses your Visa card without your permission to fund a P2P payment to themselves or an associate. They might use stolen Visa card details to fund the payment or hack into your P2P account and use your Visa card registered on the account. If you did not initiate or participate in a payment, contact your Financial Institution, and provide requested information to get your case reviewed and corrected.

  The policy requires issuers to replace funds taken from your account as the result of an unauthorized credit or debit transaction within five business days of notification.

4. What are some scenarios where the Zero Liability Policy would apply?

- A fraudster accesses a customer's Visa credit or debit card, potentially by obtaining credentials on the dark web, and subsequently funds a transaction or a payout or load of an account on a P2P app

1. Visa's Zero Liability Policy does not apply to certain commercial card and anonymous prepaid card transactions or transactions not processed by Visa. Cardholders must use care in protecting their card and notify their issuing financial institution immediately of any unauthorized use. Contact your issuer for more detail.

- A fraudster hacks into a P2P app and loads the account via the linked Visa card and sends it to another account.
- A fraudster obtains a stolen card and uses it to fund an account under their control.

5. Does Visa's Zero Liability Policy protect against Scam Fraud / Authorized Push Payment Fraud?

- In an instance of scam fraud / authorized push payment fraud, a fraudster convinces a consumer to send them funds via a P2P payment service. The victim initiates or participates in a payment from their Visa card account to fund the P2P payment. Since this is an authorized payment – it was initiated by the consumer – Visa's Zero Liability Policy does not apply. The policy solely covers unauthorized payments. Victims of scam fraud are advised to contact their account or wallet provider to report if they have been the target of authorized push payment fraud.

6. What are some scenarios where the Visa Zero Liability Policy would not apply?

- A bad actor or fraudster hacks an account and it already has funds in it that the fraudster then transfers to another account. While this is not covered by Visa's policy, consumer protection regulations may require the P2P app provider or bank to cover. For example, if your mobile payment service application account had stored funds in it that were hacked, under typical consumer regulations, the payment service application would be responsible for covering this.
- A consumer authorizes a push payment from their account after a fraudster convinces them to send money. In this simple example of authorized push payment fraud, the consumer would typically not be covered by the bank or the application provider because they authorized the payment.

7. How can consumers protect themselves from scam fraud?

- The best way for consumers to protect themselves is to be vigilant when authorizing payments and to educate themselves on potential red flags that may suggest they are the targets of a scam. Some red flags include:
  - You are contacted out of the blue by an unknown or unfamiliar individual insisting you initiate an urgent payment
    - Scammers frequently impersonate government officials, law enforcement, utility company employees, healthcare workers, and volunteers at charities or religious organizations
    - "Spoofing" refers to scenarios where a scammer mimics or uses a legitimate brand or institution to solicit funds. In some instances, this may manifest as a "me-to-me" spoof, where fraudsters trick customers into sending money to what they think are their own accounts.
  - You are instructed to initiate a payment in order to receive a prize
  - You are urged to act quickly by an individual stressing the need to initiate a payment immediately (the individual may emphasize urgency of the matter or the precariousness of a situation)
  - You are presented with an offer that sounds suspicious, or simply "too good to be true."
- In addition to being cognizant of red flags, consumers should:
  - Never share personal details, including passwords, PINs, or one-time pass codes with anyone contacting them (through e-mail, phone, text, social media, etc.) and claiming to be from a trusted company.
  - Never respond to a phone number listed in an e-mail or caller ID. Instead, use the contact details you have for the trusted company or access a "contact us" page on their trusted website.
  - Look for additional red flags in e-mails. Consumers should be cautious of e-mails containing urgent language, requests for personal or confidential information, poor grammar, misspellings, or an unrecognized / suspicious sender e-mail address.
  - Refrain from clicking on links or opening attached files
  - Regularly access their financial institution's website to learn about additional scam fraud mitigation best practices.

8. What value-added services does Visa provide enablers of A2A and P2P payments via Visa Direct[2] on Card?

- Specific risk management products supporting Visa Direct card transactions include:
  - Visa Advanced Authorization - provides global issuers with in-flight fraud risk scoring, to inform authorization decisions.
  - Visa Risk Manager - uses rapid insights of Visa Advanced Authorization and provides card issuers the ability to put in place rules to prevent approvals of fraud transactions.
  - Visa 3-D Secure 2.0 - enables the exchange of data between the merchant, card issuer and, when necessary, the consumer, to validate that the transaction is being initiated by the rightful owner
  - Visa Token Service - a security technology from Visa, replaces sensitive account information, such as the 16-digit primary account number, with a unique digital identifier called a token.
  - Card Verification Value - a unique check value encoded on the card to validate card information during the authorization process.
  - Address Verification Service - a feature that allows card-not-present merchants to check a Visa cardholder's billing address (where available).
- Visa continues to develop new products and services to protect the ecosystem. Currently we're working on a new solution, Account Name Inquiry (ANI), which will enable a transaction originator, merchant, or money movement operator to check that the name provided by their customer matches the name registered at the issuing bank.[3] This requires issuers to share the account holder name with Visa to do the match or the issuer can perform the match on their side and determine if there's an inconsistency. ANI can provide a result of "full match," "partial match," or "no match."
  - *Example*: A fraudster, Bob, unlawfully obtains Sarah's card number and credentials. Bob logs into his digital wallet and adds Sarah's card credentials with the intention of initiating an Account Funding Transaction (AFT) to fund his digital wallet. The digital wallet provider, however, could use ANI to conduct a name check. The name check reveals that the name on Sarah's account does not match Bob's name on his wallet account. The wallet provider could use this information to prevent Bob from adding Sarah's card to the wallet and stealing funds from her card account.
  - *Example*: A fraudster, Bill, takes over Claudia's brokerage account at a brokerage firm and attempts to register his card to transfer funds to his own account. The brokerage firm could use ANI to discover that the name on Bill's card does not match Claudia's name on the account. Identifying the mismatch, the brokerage firm could use ANI to stop the fraudulent payout
  - *Example*: A fraudster using the alias "Frank" connects with Arielle on a dating application. Although "Frank" is unwilling to meet Arielle in person, they speak frequently over social media applications. Having won her trust, "Frank" informs Arielle that he recently made a risky investment, and while he expects to make a significant return, he needs funds now to cover some immediate expenses and sends her his card number where she should direct the funds. Arielle agrees to send the funds using her Payment Service Provider (PSP), which requires her to enter the card number and the name of her intended recipient "Frank". The PSP could use ANI to check "Frank's" name against the details held on his card account. The PSP then notifies Arielle that the name of the intended recipient, "Frank," does not match with the name on the account and asks her to check she is paying the right person before going ahead.

9. What value added services does Visa provide for domestic A2A or P2P payments using Visa Direct NOT on a card (i.e. accounts and wallets)?

- Visa Direct account to account domestic payments primarily use card rails today and do not use RTPs or ACH networks. Cross-border P2P that utilizes Visa Direct may involve card rails as well for the funding of the payment.
- Therefore, the same risk management products for Visa Direct account to account payments apply to payouts through cards or not on cards if the funding is done using card rails.
- For those Visa Direct cross-border transactions that utilize RTP or ACH networks for the first or last mile, then, Visa risk products do not apply but consumer protections apply in accordance with country regulations for electronic payments.
- We continue to develop and explore services we can provide on all networks.

2. Visa Direct clients and participants should always consult and seek approval from their internal compliance teams on sanctions screening controls and processes, and are solely responsible for their own compliance with applicable laws and regulations. Optional compliance controls and risk management tools and services are provided solely for the convenience of sending acquirers, service providers, merchants, and recipient issuers / the Visa Direct clients and participants, and Visa makes no warranties with respect to them or their results. Visa Direct clients and participants are solely responsible for their own compliance with applicable laws and regulations.

3. This is intended for illustrative purposes only. It contains depictions of a product currently in the process of deployment, and should be understood as a representation of the potential features of the fully-deployed product. The final version of this product may not contain all of the features described in this document.