RICHTER GUARDIAN

RGSA 04-19-24-01
Date: April 19, 2024

What is Authorized Push Payment Fraud?

INTRODUCTION

Authorized push payments involve an account holder granting permission to their bank or payment service to transfer funds directly from their account to another account. The payer usually triggers this transaction using services like online banking, phone banking, or peer-to-peer payment platforms.

Authorized push payment (APP) fraud, also known as bank transfer scams or authorised bank transfer fraud, occurs when a victim is tricked into authorizing a payment to an account controlled by a scammer.

Unlike unauthorized transactions where a fraudster gains access to someone's account without permission, in APP fraud, the victim is deceived into willingly making the payment, often believing they are paying a legitimate entity or individual.

HOW DOES APP FRAUD HAPPEN?

Authorized push payment fraud can happen in various ways.

1. **Advance Fee Scams:** The victims are asked to pay a fee to access a service or a prize, which are never delivered. For example, a scammer may impersonate a lottery organization, and will withhold the prize until an administrative fee is paid. When the payment is made, the victim never receives the reward.
2. **Impersonation**: The scammer poses as a trusted entity, such as a bank, government agency, utility company, or even a friend or family member, and requests payment for a fake invoice, overdue bill, or urgent situation.
3. **Fake Services or Goods:** The victim pays for goods or services that are never delivered or are significantly different from what was advertised. The scammer may set up a fake online store, auction, or classified ad to lure victims.
4. **Social Engineering**: The scammer manipulates the victim through psychological tactics, exploiting emotions like fear, urgency, or greed to coerce them into making the payment.
5. **Business Email Compromise (BEC):** Scammers compromise email accounts of businesses or individuals, or create lookalike accounts, and use them to request payments from employees, clients, or partners, often by impersonating company executives or vendors.
6. **Invoice Fraud:** The scammer pretends to be a vendor and sends fake invoices to the business. The invoice may request payment for goods or services that were never delivered.

PREVENTION

We recommend the following measures to mitigate the risks of authorized push payment fraud.

1. **Verify the authenticity of requests for payments** – ensure that the request for payment is legitimate by confirming the identity of the individual, organization or service you are initiating a payment for. If the payment is sent to an organization, check the organization's website and contact their phone number to confirm the request.
2. **Establish payment protocols** – establish clear protocols within your organization that outline how to properly authorize payments. Ensure relevant employees are aware of these protocols and procedures.
3. **Monitor transactions** – check your accounts to identify any unusual activity that could indicate fraud.

RGSA 04-19-24-01
Date: April 19, 2024

HOW RICHTER GUARDIAN CAN HELP YOU

To combat APP fraud, it's essential for individuals and businesses to remain vigilant and verify the authenticity of requests for payments. We understand that It can be difficult to approach this alone.

- Call us or send us an email at: +1 844-908-3950 and support@richterguardian.com if you are unsure. Connect with our cyber concierge to verify the legitimacy of a situation.
- Transunion identity protection is included on our platform. Transunion identity protection will alert you of any unusual activity on your credit monitoring report that could indicate fraud.

CONTACT US

Have a quick question? Send us an email.
Email: support@richterguardian.com

Phone number: +1 844.908.3950
Monday to Friday 9 a.m. to 5 p.m. (Eastern Time)

Need assistance upgrading your device?
Schedule a session with us by clicking here