Carat from fiserv.

Closed loop prepaid

Gift Solutions
Fraud and Risk account takeover

Consumer account fraud, phishing and social engineering scams

Fraud synopsis

As a form of identity theft, compromised user accounts may contain credit, gift or loyalty information used to make eCommerce purchases or store brand credit. This data remains a prime target for threat actors due to their wide adoption and clear line to monetary gain.

Scheme Tactics, Techniques and Procedures (TTP) include a variety of methods to gain unauthorized access to consumer accounts.

The scheme includes specific patterns:

- Social engineering is the use of deception, through manipulation of human behavior, to target and trick you into divulging confidential or personal information and use it for fraudulent purposes[1]
- Phishing, in all sub-forms, through phone, email, and social media serves as a conduit for bad actors to seek targets. A targeted individual may divulge user credentials, payment card information or other personal details
- Credential cracking or credential stuffing attacks can combine known and unknown information to produce the highest likelihood of successfully guessing user credentials
- Compromised accounts may be skimmed for information or used to attack adjacent user targets by established trust through connected accounts

Account takeover fraud (ATO)

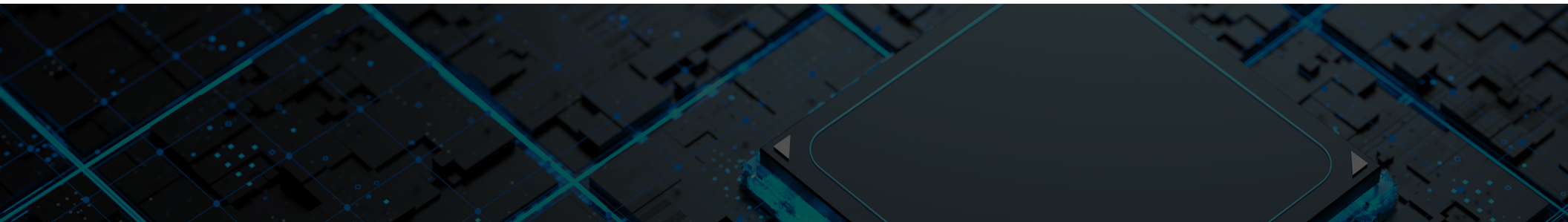
ATO occurs when a threat actor gains unauthorized access and assumes control over a user account. Often consumers are unaware of the potential for being a target of phishing or collateral damage in a credential stuffing event.

User accounts, which may include loyalty or stored payment information, should use a Multi-factor Authentication (MFA) method. These methods should include a new factor in validating the user such as, authenticator application or One Time Passcode (OTP), upon login.

Fiserv recommends that you take the following proactive steps:

Improve access control

- Enforce strong MFA for applications where a user may conduct financial transactions
- Require regular password resets
- Enforce long, complex passwords that are not easily guessable



Validate account changes

- Account changes concerning contact information or payment details should validate the intended user is making the change by
  - Multifactor authentication of ownership and
  - User notification through both SMS and Email concerning the change

Reduce exposure

- Obfuscate all payment details that are vaulted or stored within the app
- Set or establish limits and controls to user activity by creating thresholds based on financial impact, such as abnormal spending patterns or concentrated account merges
- Create a process to identify and record confirmed fraud with the intention to analyze the data to further develop and enhance controls
- Review Social Engineering tactics with call centers and operators to best understand TTP

Connect with us

Contact your Fiserv account manager to learn more.
Or email us at GiftSolutions@Fiserv.com.

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today.

Visit **Carat.Fiserv.com** to learn more.

Learn more with protected voices >

Carat from fiserv.