What is an Account Takeover (ATO)?

Account takeover is an attack in which cybercriminals take ownership of online accounts using stolen passwords and usernames. These cybercriminals then use these credentials to commit fraud. These bad actors purchase cardholders' Personally Identifiable Information (PII) via the dark web, often obtained from data breaches, or gain the data from social engineering, such as phishing, vishing, or smishing attacks (detailed below). Stolen PII (e.g., name, address, email, phone number, date of birth, business name, cellphone provider, social media and login accounts and passwords) provides the necessary credentials for a fraudster to pose as a cardholder.

With this information fraudsters can engage with the cardholder's financial organization and make changes to accounts or card settings to execute fraud. They may make demographic changes (e.g., phone numbers, emails, passcodes), or apply for increased limits, Personal Identification Number (PIN) changes and/or travel exemptions to suppress or interfere with our fraud-monitoring tools.

The activities described above are most commonly associated with merchant data breaches described in media reports. However, in the case of account takeover, the stolen data is not obtained from a payment system.

Common fraud schemes that can contribute to Account Takeover

Skimming and Malware

Skimming and deployment of POS terminal malware continue to be widespread methods for stealing data. Smaller, local merchants are now more likely to be compromised than in years past. Stolen data, which is collected using POS malware, is passed to criminal networks through remote, wireless technologies with increasing speed. By reacting to fraud events quickly, your organization can significantly mitigate losses.

Phishing

The prevalence of phishing (tricking cardholders into revealing confidential information) and its variants continue to rise. Phishing schemes are becoming more targeted and more difficult to identify than in the past. Instead of using only suspicious links in poorly designed emails, phishing emails are mimicking legitimate websites and appear more polished and credible. The

use of web address shortening tools, such as TinyURL, make detection of suspicious links more difficult, even by savvy users. It is important to remind cardholders to safeguard their financial data and their online banking credentials against criminals trying to harvest it.

Vishing and Smishing

Smishing and Vishing schemes use sophisticated methods combined with social engineering to deceive cardholders into revealing critical information and disregarding legitimate fraud warnings.

Smishing is the fraudulent practice of sending text messages claiming to be from reputable companies to induce individuals to reveal personal information, such as passwords or credit card numbers.

Vishing is the fraudulent practice of making phone calls or leaving voice messages claiming to be from reputable companies to induce individuals to reveal personal information, such as bank details and credit card numbers. Cardholders may be sent a voice or text message with transaction details and requesting the cardholders confirm. When they respond, they may be questioned for account details, or they may be asked to call back a number to provide account information. In some instances, they are sent a onetime passcode (OTP). The caller or text message then instructs the cardholder to reply “No Fraud” to text/voice messages.
It is important to be on the lookout for these kinds of fraudulent messages that disguise themselves as legitimate fraud notifications. These schemes use sophisticated methods combined with social engineering to deceive cardholders into revealing critical information and disregarding legitimate fraud warnings. Additional red flags of note include hyperlinks and grammatical and punctuation mistakes.

Malicious Software

Malicious software, including software which compromises account-holder computers locally via Man-in-theBrowser (MitB) attacks, are a significant threat to the security of financial data. Man-in-the-Browser attacks install malicious software in the background via “drive by download.” This malware monitors and hijacks user web sessions to then transfer funds or harvest payment cards and online banking credentials, while redirecting the legitimate cardholder to a fictitious error page. This type of malware often deploys automatically when a user visits a compromised website.

Maintaining a secure, up-to-date operating system, along with robust security and anti-malware software, is a critical first step in preventing this type of fraud. Availability and deployment of automation and crime-ware is increasing in the card fraud world. Both all-in-one malware packages, designed to compromise computer systems (e.g., Zeus, Citadel, Tilon), as well as individual tools able to crack passwords and to automatically carry out brute force attacks, are available for purchase on underground websites and on criminal forums. Heavy reliance on one type of security tool or on older tools could lead to more fraud loss. We recommend a dynamic, multi-layered detection and prevention strategy.

Non-card Related Scams That Can Lead to Account Takeover

Stay on top of any large events that are coming up and be on the lookout for scams/schemes. Fraudsters like to take advantage of what is going on in the world, such as tax season, the Olympic games, and national sporting events, which are prime times for criminals to take over cardholder identities. As result this can lead to account takeover, loans being opened in their names, cards being used for fraud, etc.

Explosion of scams such as imposter, online shopping, lottery, and romance scams are very common as well. Some of the scams are similar to those used in other countries, which target victims by SMS/text messages and often falsely direct the recipient to provide personal identifiable information (PII) and/or to make a payment for an unpaid parcel allegedly pending delivery.

Visa has some new information about Threat Actors Exploit eSIM Technology to Conduct Account Takeover, which embeds users' SIM cards for their mobile smartphones within the device itself rather than requiring a physical, removable SIM chip. This technique reveals threat actors' interest in continuing to find ways to exploit new technologies to gain access to sensitive victim information, particularly financial account information or credentials. These can lead to Phishing and Vishing attacks. It is important for cardholder to stay diligent about odd looking text senders, emails, etc.

Recommendations:

Cardholder Recommendations

Remind cardholders to be aware of what information they are choosing to submit online and never easily provide their personal information.

If a consumer is concerned about an automated message, they should not respond to the call, text, or emails. They should contact the company in question using the official customer service number on their own card or contact information listed on the company's legitimate website. They should not contact any number provided by the fraud call or message and should not click on links in text messages.

If they are responding to your FI's fraud alert message, for a transaction they do not recognize they should confirm fraud or if unsure about the transaction call the bank directly. They should never reply NO fraud for a transaction they do not recognize.

Cardholders should always keep two-factor authentication codes private. Do not provide them via phone, text, or email. These codes should only be used to sign into the banking, merchant, or payment account when the consumer is trying to access it. One time passcode (OTP) may be used by Fis in order to validate who they are but should only be shared if the cardholder is the one calling into us, not if they answer an incoming call.

Recommendations for Your Organization

Place a banner on your institution's online banking website after cardholder authenticates their password indicating that customers will never be asked for full social security numbers, PINs, or any other PII (Personal Identifying Information)".

Place a message like this on your phone system in place of "hold" music. In cases of suspected fraud, notify local authorities and the impacted networks. One time passcode (OTP) may be used by Fis in order to validate who they are but should only be shared if the cardholder is the one calling in, not if they answer an incoming call.

- Place a banner within the online banking profiles after SSO or log on credentials have been applied and verified. Main page of the websites for most institutions are public domain and we may provide strategy or details to fraudsters gathering their reconnaissance to execute the fraud.

- If needed, add One-time Passcode (OTP) authentication tool as an additional layer security. (**Step Up with NO FALLBACK)**

Recommend that your cardholders sign out of all financial apps on their phones. If possible have them enable PIN, Face or fingerprint recognition. This way if any fraudster gets ahold of the physical phone or hacks into the phone, they will have a much harder time gaining access to financial information.

- Enabling MFA Authentication (Multi-factor Authentication) as another layer of security, to assist with securing the account and proactively mitigating such takeovers.

If the fraudster is impersonating your organization by using a number or caller ID that appears to be valid, you should contact your service provider.
Make sure authentication factors on the database are set to 100% authentication match on IVR options (this is to validate the caller when changing limits, PINs, exemptions etc.).
When setting rules for the current trend, include the Ignore All Exemptions and Restrict Card options.

If CardValet® or CardHub® is involved, contact your account executive to request temporary suspension of new enrollments.
We highly recommend your cardholders request a consumer credit report once a year through one of the three main credit reporting agencies - Experian, Equifax, TransUnion - or via Annualcreditreport.com