Account Takeover (ATO)

<h2>GUIDE.SUMMARY What <ul> An Account Takeover (ATO) is any event where an unauthorized third party is able to access a member's account. Perpetrators of Account Takeover fraud have varied motives, but commonly want to use an established accounts tenure and history of activity, to appear trusted and reputable to any other members they interact with. Some typical ATO scenarios: <ul> Selling non-existent items (receiving & exiting funds without delivering), selling counterfeits, stolen goods (triangulation fraud) Buying items from sellers using stolen financials or illicit funds Spamming other users with unsolicited messages through our Member to Member (M2M) system   How <ul> A fraudster could have obtained a user's credentials through various avenues. Common methods are: Phishing or spoof emails (responded or provided information that could be used to access), external data breaches (same credentials exposed from somewhere else also used on eBay), social engineering, malware, and credential stuffing. There are several ways this can occur and various actions the third party may take. We actively search for such activity and restrict these accounts until the actual owner can verify themselves. This ensures the safety of their information as well as the safety of our community.   </h2><h2>GUIDE.RELATED_LINKS Help pages <ul> Protecting your account
 https://www.ebay.com/help/protecting-account/account/protecting-account?id=4192
   Tips for keeping your eBay account secure
 https://www.ebay.com/help/protecting-account/account/tips-keeping-ebay-account-secure?id=4872
   eBay's Security Center
 http://pages.ebay.com/securitycenter/ind

ex.html
   Get help with a hacked account
 https://www.ebay.com/help/protecting-account/securing-account/get-help-hacked-account?id=4196
   Avoiding payment problems for items you've sold
 https://www.ebay.com/help/selling/avoiding-payment-problems/avoiding-payment-problems-items-youve-sold?id=4660
   Protecting yourself against gift card scams
 https://www.ebay.com/help/paying-items/buying/protecting-gift-card-scams?id=5156 CSKB articles <ul> Account safety Spoof emails/phone calls - Possible scam tactics and how to avoid them Hard verification Spendable funds Errors, Unauthorized transaction policy & process Solutions <ul> Ato issue resolved (self-restored/regained access)   </h2><h2>GUIDE.TALKING_POINTS How did the ATO happen? Was your system hacked? ATOs most commonly occur when a user responds to

a spoof email, giving information that could be used to access an account. Spoof emails claim to be from a trustworthy source like eBay and ask you to provide personal account information such as passwords and payment details. Often, the email asks you to click on a link and sign in to a fake website. You can forward questionable emails to spoof@ebay.com. See Spoof emails - Possible email scam tactics and how to avoid them for more information. Other methods include the email being compromised, malware on the device, and social engineering via text messages and social media. Seller had ATO - buyer has already paid <ul> An unauthorized third party may have accessed the sellers account to list the item you bid on/purchased. The item has now been removed from the site and the transaction has been cancelled. If you have already paid for the item, we ask that you visit http://resolutioncenter.ebay.com to open a request. If you do not qualify for eBays protection, please immediately contact the payment service used to request a refund. If you have not paid for your item please consider this transaction canceled and do not send payment.   Buyer had ATO - seller has already shipped <ul> An unauthorized third party may have accessed the buyers account to purchase the item you listed. Please consider this transaction has been cancelled and do not ship the item. If you have already shipped the item and it was paid via Credit or Debit card, Apple Pay, Google Pay, the seller should upload tracking as they will be protected provided they ship to a confirmed address. If you have adhered fully to eBay seller protection guidelines, and unless instructed otherwise by eBay or PayPal, you can retain the funds received. If you have already shipped the item using payment other than Credit or Debit card, Apple Pay, Google Pay or PayPal, we recommend you contact your local law enforcement and provide them with the details.

We work closely with all law enforcement agencies. How to prevent this from happening again <ul> Sign in only from eBay.com. Don't click on links from your email account. You can confirm an email has come from eBay by checking that a copy has also been sent to your eBay messages. If not, then don't respond to it. Other ways you can protect yourself include: <ul> Have frequent virus and spyware scans. Enable multi factor authentication. Review the contact information on your account and keep it up to date at all times. Never respond to a user that you don't recall dealing with, or regarding an item you are not selling. Keep in mind that eBay will not ask you to sign in to view an individual item. Regularly update your passwords and vary them between accounts. For practical advice, go to: http://pages.ebay.com/help/newtoebay/account_protection.html   Was the person who accessed my account without permission able to get my financial information? Financial information is stored on a separate and secure server and cannot be viewed by anyone, even if they accessed your eBay account. How did you discover the unauthorized activity? eBay has many security and investigation tools and procedures that led us to this action. Are you going to find the person who accessed my account without permission? Contacting law enforcement <ul> It can be very challenging to identify the individual(s) who compromised your account, but we do sometimes work with law enforcement and agencies in these matters. If you like, you can report an issue to your local law enforcement agency. We can't initiate a third party report on your behalf, but we will be happy to assist them in their investigation. They can use your Username as a case reference and contact us at:
 http://pages.ebay.com/

securitycenter/LawEnforcementCenter.html User is reporting unauthorized use of spendable funds <ul> Review for ATO and action per workflow. If user is claiming any use of eBay spendable funds for item purchases, shipping labels or refunds to their customers, please route the contact to e2M Account>Account Takeover. For all other reports of unauthorized payments, the individual should be advised to contact their financial institution. User is asking why they must complete (Hard) verification <ul> Without being verified, the user can't regain access to their account. Verification allows us to confirm that control of the account is only given to the true account holder. Users feel reassured that we take account security seriously. We aren't just giving control of the account to the first person who contacts us.   Internal Information <ul> Third parties (fraudsters) have begun contacting CS to try to regain access to the account, as well as phish for information about how they can potentially get by our verification methods.   </h2><h2>GUIDE.DETAILED_INFORMATION Related Issues Internal Information <ul> See the Trust & Safety Issues Directory for more information. Do not share the issue number with customers. <table border="1" cellpadding="2" cellspacing="0"> <tbody> <tr> <td>Issue</td> <td>Name</td> </tr> <tr> <td>12</td> <td>ATO Restoration: Listing / Bidding / Email Block</td> </tr> <tr> <td>34</td> <td>ATO Self Remedy</td> </tr> <tr> <td>57</td> <td>ATO selling or bidding velocity issue</td> </tr> <tr> <td>180</td> <td>Suspicious sign-in detected DO NOT CLOSE</td> </tr> <tr> <td>539</td> <td>eMBG Use Only For 45 days Buyer Claims may be ATO selling</td> </tr> <tr> <td>629</td> <td>RPO Hi Confidence ATO

Comp</td> </tr> </tbody> </table>   </h2>