PROTECTING INDIVIDUALS FROM ACCOUNT TAKEOVER FRAUD

Account takeover fraud attacks are one of the fastest-growing threats in financial services, and individuals are often the most vulnerable. When criminals gain access to a customer's account, the consequences can range from customers losing most of their funds to missed bill payments to emotional harm.

By guiding customers toward straightforward, proactive steps to help prevent and mitigate account takeover fraud, financial institutions can help reduce risk, build customer trust and create a stronger defense against evolving fraud tactics. Prevention starts with awareness – and every layer counts.

EDUCATING CUSTOMERS ABOUT SECURING THEIR PERSONAL INFORMATION AND ACCOUNT CREDENTIALS

When it comes to protecting individuals, account takeover fraud prevention can begin before a criminal tries to log in. By educating customers on simple habits to reduce exposure of their personal information and account credentials, financial institutions can help mitigate account takeover fraud risks before they materialize.

Criminals often use urgency to pressure victims into sharing sensitive details. Emails, texts or calls claiming "immediate action required" or threatening account closure are common red flags. Financial institutions should educate customers about social engineering and scams, such as providing guidance about the importance of pausing and verifying the communication source and never clicking suspicious links or sharing account credentials over the phone. Keeping customers informed about common and emerging scam types can be helpful as criminals constantly shift tactics and schemes to deceive victims.

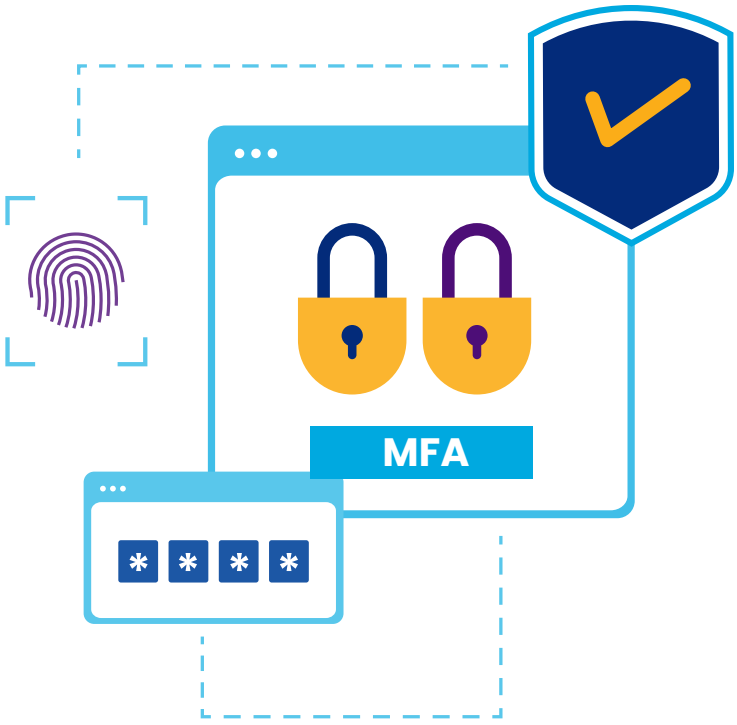
Financial institutions can make customers aware of the risks of sharing personal information on social media. Details such as a customer's pet's name, favorite sports team or high school mascot may seem harmless, but these details may be used by criminals looking for answers to security questions or password clues. Financial institutions can advise customers to limit the amount of personal information they share online to help protect their personal data and accounts.

PROTECTING INDIVIDUALS FROM ACCOUNT TAKEOVER FRAUD

Using one email for financial services and a different one for social media, shopping or personal communication helps add a layer of protection. If a customer's non-financial email account is compromised, it will not automatically expose account credentials. By promoting these practical steps, financial institutions can help individuals reduce the risks of harvesting, when criminals seek account credentials and other personal information to impersonate the account holder.

STRENGTHENING HOW INDIVIDUALS ACCESS THEIR ACCOUNTS

Financial institutions can help strengthen customer protection by educating them on more secure ways to access and manage their accounts. This includes encouraging customers to secure the devices they use for payments and transactions, such as locking phones and tablets with a password or facial recognition. Customers also can avoid installing banking or payment apps on shared devices, such as those used by children for streaming or games. These steps help make unauthorized access much more difficult.



Financial institutions also can promote the use of Multi-Factor Authentication (MFA) wherever it is available – and not just for banking. MFA adds an extra layer of protection by requiring more than one step to verify identity, such as a password plus a one-time code or a passkey. Customers can strengthen their login security further by using an authenticator app, which provides more reliable verification than text messages, or choosing to use a physical security device if they prefer an option that is not tied to their phone.

Additionally, financial institutions can highlight the benefits of biometric authentication to access a financial institution's app or site, such as fingerprint or facial recognition, which offers a strong balance of security and convenience. These tools help ensure that only the legitimate account owner can access sensitive financial information while still providing a smooth, user-friendly experience.

PROTECTING INDIVIDUALS FROM ACCOUNT TAKEOVER FRAUD

THE LAST LINE OF DEFENSE

Financial institutions can emphasize the importance of enabling account and transaction notifications for identifying account takeover fraud risks. Real-time alerts about account changes or unusual transactions give customers immediate visibility into what might be suspicious activity. These notifications allow quick action if something looks suspicious, helping stop fraud before it escalates. However, real-time notifications cannot be relied on in isolation. Criminals perpetrating account takeover fraud often will make changes to the user's account information or contact details, preventing financial institutions from being able to communicate with the legitimate account owner. Aside from enabling alerts, financial institutions can encourage individuals to proactively review their account activity regularly. Even with alerts, these periodic checks help catch smaller fraudulent transactions that might slip through automated notifications.

Lastly, financial institutions can consider providing guidance to customers about the benefits of maintaining separate accounts for different purposes, such as one for bill payments, another for peer-to-peer transfers and a primary account for savings. This would limit potential losses if/when account takeover fraud does occur. By combining real-time notifications, regular monitoring and account segmentation, financial institutions can empower customers to detect and stop fraud before it escalates.

CONCLUSION: EMPOWERING INDIVIDUALS TO PREVENT ACCOUNT TAKEOVER FRAUD

By encouraging individuals to protect personal information, such as avoiding oversharing on social media and spotting suspicious communications, financial institutions help reduce the chances of credential harvesting. Secure access methods, like biometrics and multi-factor authentication (MFA), add critical layers of defense that make unauthorized entry more difficult.

Educating customers about the benefits of enabling real-time alerts, periodic monitoring and account segmentation ensures individuals can detect unusual activity quickly and limit exposure if an account is compromised.

PROTECTING INDIVIDUALS FROM ACCOUNT TAKEOVER FRAUD

These steps are actionable and can be highly effective. When financial institutions take an active role in educating and empowering individuals, they strengthen trust and create a united front against fraud. Account takeover fraud prevention is an ongoing effort as criminals evolve their tactics, so institutions can continue to reinforce these best practices and adapt strategies to stay ahead. Together, institutions and their individual customers can build a strong shield against account takeover fraud.

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.