Supporting Your Financial Safety: Actionable Steps After Financial Fraud

give anhour® Mental Health. For Life.

FINRA Investor Education FOUNDATION

If someone has been financially scammed, taking quick and decisive action is crucial. These steps help mitigate the damage and prevent further fraudulent activity.

Contact the Financial Institution or Service Provider

- Immediately notify the bank, credit card company or other financial institution where the funds were withdrawn. They may be able to freeze accounts, reverse unauthorized transactions, or provide temporary security measures.

Document Everything and Report to Authorities,

- Keep detailed records of all interactions with the scammer (emails, phone calls, text messages, etc.), including the date and time of communications and any financial transactions.
- Collect screenshots, transaction details, or any receipts from the scam.
- Report the scam, to the authorities (IC3.gov, FTC, FBI, police,)

Change Passwords and Secure Accounts

- Immediately change passwords for any online accounts, especially for banking, email, and social media. Enable two-factor authentication wherever possible.
- If the scam involved an online service, consider contacting the service provider to flag any changes or breaches in your account.

Place Fraud Alerts or a Credit Freeze

- Contact one of the three major credit bureaus (Experian, Equifax, or TransUnion) to place a fraud alert or a credit freeze. This will prevent further unauthorized use of your personal information.
- Regularly check your credit report for any new, unauthorized accounts or activity.

Report to Consumer Protection Agencies

- In the U.S., you can also report the scam to Better Business Bureau (BBB), or relevant consumer protection agencies in your area. This can help raise awareness and prevent others from being victimized by the same scam.

Seek Legal Advice or Support

- Depending on the nature and scale of the scam, it may be helpful to consult with an attorney or legal aid services for advice on how to protect your rights or pursue legal action.

Consider Identity Theft Protection

- If sensitive information was compromised, consider signing up for identity theft protection services that monitor your personal information and provide assistance in case of further fraud.

Alert Friends, Family and Colleagues

- Inform those around you about the scam so they can be vigilant and avoid being victimized by similar schemes.

Review and Strengthen Your Personal Security Measures

- Going forward, be cautious about unsolicited phone calls, emails, or messages. Research any unfamiliar contacts or offers, and always verify before providing personal or financial details.

www.giveanhour.com/financial-fraud