Account security: prepare and be aware

Financial fraud has become quite sophisticated. Fraudsters are more bold and expanding into areas previously untouched, such as mutual fund accounts. DWS has implemented a variety of controls and governance in line with other mutual fund companies; however, the risk of fraud remains a probable concern. Below are tips to consider, along with critical steps for you to implement and remain vigilant to reduce risk of fraud on your account.

Stay aware

It is critical that you periodically review your account activity, which includes reviewing all mail and email from DWS in a timely manner. Your account statements, transaction confirmations and account-related notices could reveal unauthorized activity on your account, such as redemption, change in address, change in bank accounts and online account access you did not request.

Accounts without activity for a prolonged time are more susceptible to fraud.

Please notify us immediately upon an account owner's passing so we can take the necessary steps to help protect the account.

Action to take

Contact us immediately if you are unsure of information you receive from DWS or you suspect unauthorized activity.

Our service representatives can be reached at (800) 728-3337, Monday – Friday, 7 a.m. to 6 p.m. Central time.

Help us help you

If DWS investigates suspected unauthorized activity in your account, please cooperate with us. We may ask you to file a police report or provide a statement of facts.

It may take some time and effort to complete our investigation to ensure proper resolution. We may contact you for additional information.

Critical steps

Physical documents

_ Promptly retrieve and review your mail.
_ If you intend to be away for an extended period, use the U.S. Postal Service or your respective country's postal service for "hold mail" options. Fraudsters sometimes look to identify homes that appear unoccupied and where mail is accumulating.
_ Do not throw in the trash documents that contain account numbers, Social Security number, or other personal information that may assist a fraudster. Examples include account statements, notices, transaction confirmations, credit card offers, bank statements, tax documents or junk mail containing personal information. Shred these documents instead; however, if not an option, identity theft protection stamps, rollers or markers could be used to block out personal and confidential information.
_ Immediately report suspected mail theft or tampering to the United States Postal Inspection Service, or your respective country's postal service.

Consider paperless delivery

_ If you choose this option, DWS will notify you by email when your statements, tax forms and other documents are available to be accessed through secure login.
_ With paperless delivery, you don't have to worry about shredding papers, delivery is faster and documents will

never get lost in the mail. However, ensure you protect your online accounts. The "Online Accounts" section of this document provides tips to help you.

Online accounts

Create a smart password

_ Create a unique password only for your DWS account, such as IH8broCColi!. In this example we used a long password combining upper and lower case letters, numbers and symbols. Update your password perhaps once every few months, but choose a new password substantially different than the previous password.

Protect account information

_ Store your DWS.com user name and password in a secure place, not on the device you use to access your DWS account. Do not share this information with others. If you allow someone to access your account information, any activities they perform may be considered authorized, so remain vigilant and review your account activity often.

Keep your computer secure

_ Use the latest operating system and respond to software updates promptly. Activate security features, such as pop-up blockers. Install antivirus software that detects and removes malicious software from your computer. Avoid using public computers and Wi-Fi to access any of your accounts.

Watch for "phishing."

Fraudsters have been known to send messages that appear to be from a reputable company such as DWS requesting that you send or confirm personal information such as passwords, credit card numbers or even Social Security numbers. This is known as "phishing."

_ DWS will never send you an email asking for your Social Security number, account numbers or passwords.

_ If you don't recognize the sender or are not expecting an email, don't click on it, delete it.

_ Responding or clicking on links within these messages may expose your personal and/or account-related information. DWS may at times call a fund shareholder to clarify information, such as a pending transaction request. If you receive such a call and are unsure if it is valid, please end the call and call Shareholder Services at (800) 728-3337 to verify.

DWS takes your account security seriously and hopes you will consider these tips and steps to help protect your account.

The Financial Industry Regulatory Authority (FINRA) offers a wealth of information and resources to help you recognize and address the potential risks of financial fraud. Visit FINRA.org to learn more.

DWS Distributors, Inc.
222 South Riverside Plaza Chicago, IL 60606
www.dws.com
Tel +1 (800) 621-1148