DWS Account Security Program

As a trusted partner in serving your investment needs, DWS takes account security seriously. We developed the **DWS Account Security Program** to explain what DWS does to help protect your account(s) and what you can do to reduce the risk of fraud. Protecting your account is a shared responsibility, and small steps can make a meaningful difference.

Contact DWS immediately at (800) 728-3337, Monday - Friday, 7 a.m. to 6 p.m. Central Time, if you suspect unauthorized account activity, notice errors or discrepancies, stop receiving statements, or believe your personal information may have been compromised.

Losses related to unauthorized activity or fraud may be eligible for recovery if you follow the DWS Account Security Program and report concerns promptly. If you do not follow these practices, losses may be deemed ineligible for recovery.

Monitor your account(s)

DWS sends periodic statements and transaction confirmations by electronic delivery or U.S. Mail, depending on your delivery preference.

Regardless of your delivery preference, DWS will send paper confirmations to your address of record by U.S. Mail when certain changes are made to your account(s), including:
(1) establishment of online access; (2) changes to bank account information; and (3) updates to your email address or U.S. postal address.

Changes to your address of record or banking information cannot be used to receive redemption proceeds for 15 calendar days after the change is received in good order and updated on your account(s).

Open Your Mail – Review statements, transaction confirmations, and account notices as soon as you receive them. These communications may help you spot unauthorized activity quickly.

Not Receiving Statements? – If you are not receiving your DWS quarterly account statements or transaction confirmations, contact us immediately.

Your Contact Information – Keep your mailing address, email address, and phone number current so DWS can reach you if there is a question about your account.

Online Access – If you have DWS online account access, log in regularly and review your account activity. Report anything you do not recognize immediately.

Credit Monitoring – Review your credit report from time to time for signs of suspicious activity or identity theft.

Protect your online account(s)

Add a "Trusted Contact" - A trusted contact is someone DWS may contact if we are concerned about fraud, financial abuse, or unauthorized transactions. This person is not authorized to transact on, or make changes to, your account(s). Contact DWS Shareholder Services at (800) 728-3337 for details.

Establish Online Access – Creating and maintaining access at dws.com or through the **DWS Direct USA app** can help you monitor your account(s) and identify unauthorized activity sooner. DWS uses multifactor authentication to help protect online access.

Use Unique Passwords – Use a password for your DWS login that you do not use anywhere else. Change it periodically and avoid saving it where others can see it.

Keep Your Information Secure – Never share your username, password, verification codes, or account access information. If you give someone access to your account information, their activity may be treated as authorized.

Watch for phishing, smishing, and AI-assisted fraud

Phishing emails and **smishing** text messages are attempts to trick you into sharing sensitive information, such as usernames, passwords, verification codes, or Social Security numbers. Scammers may use artificial intelligence (AI) to make messages sound more realistic or urgent. **DWS will never ask for your account password.**

If you receive a suspicious email, text message, phone call, or other communication about your DWS account(s), **contact us immediately.** DWS may apply heightened monitoring to help protect your account(s).

_ Be cautious of messages that create urgency, ask you to click a link, request personal information, or ask you to approve a transaction you did not request.
_ Do not reply to suspicious messages, open attachments, or click links. These actions may expose your personal or account-related information.
_ Access your DWS online account(s) only by typing dws.com directly into your browser or using a bookmark you created. Never access your DWS online account(s) from a link in a pop-up, email, or text message that seems suspicious.

Keep your electronic devices secure

_ Keep your device operating system and software up to date and install security updates promptly.
_ Upgrade to the latest operating software system, or OS, and respond to software updates promptly
_ Turn on security features such as screen locks, pop-up blockers, and trusted security tools.
_ Log out of websites, including your DWS online account(s), when you are finished.
_ Lock your mobile phone, tablet, and computer when not in use.
_ Use antivirus or security software that helps detect and remove malicious software.
_ Avoid using public computers or public Wi-Fi to access financial accounts.

Help us help you

As part of our caller verification process, DWS may ask security questions to confirm your identity. DWS will only ask for information specific to your DWS account(s).

_ Contact us immediately if you are unsure about information you receive from DWS, suspect unauthorized activity, or become a victim of identity theft. Our service representatives can be reached at (800) 728-3337, Monday - Friday, 7 a.m. to 6 p.m. Central Time.
_ DWS may call you to verify transactions or updates that you requested. If you are unsure whether a call is valid, end the call and contact Shareholder Services using the number above.
_ If DWS suspects unauthorized activity, please cooperate with us while we review the matter. Return our calls promptly, contact us if you receive written notice that we are trying to reach you, and provide requested information such as a police report or statement of facts, if applicable.
_ Follow DWS's recommendations for safeguarding your account(s) at all times.

All reported concerns will be reviewed to determine program applicability and eligibility for recovery. Failure to report unauthorized activity promptly after notice is sent to you may result in losses being deemed ineligible for recovery.

Additional resources:

Visit the DWS Investor Resource Center at the following link and scroll down to "Prepare and be aware":

https://www.dws.com/en-us/resources/investor-resource-center/

Other helpful links:

https://www.investor.gov/protect-your-investments/fraud/how-avoid-fraud

https://www.consumer.ftc.gov/

Be careful when using checks

Scammers may steal checks from mailboxes. Checks include personal information such as your name, address, and account number. A stolen check may be altered, used to create counterfeit checks, or used to expose you to identity theft or fraud. Consider safer alternatives for purchases or redemption proceeds, such as adding your bank account to your DWS account, which can be completed online at dws.com.

Think Before You Share – Protect Your Credentials

Sharing login credentials with data aggregators, financial apps, agentic AI tools, or other third-party services may expose your personal and financial information and increase the risk of unauthorized access, identity theft, fraud, or account takeover. Before granting access, review the provider's privacy and security practices, use credential-free authorization when available, and monitor your accounts for suspicious activity.

Contact DWS Shareholder Services at 1-800-728-3337 Monday - Friday, 7 a.m. to 6 p.m. Central Time for more information or if you have questions about protecting your account.

This program applies only to accounts that you hold directly with the DWS mutual funds. Investments held through a financial advisor or other third-party are not eligible for this program. DWS will determine the applicability of the Account Security Program and the type and amount of any reimbursement. DWS will not cover legal or professional fees, loss of opportunity, or any indirect costs, including tax consequences, nor any amounts that are eligible for recovery from others including a depository bank or through insurance. We may require that you provide a police report, and sign a release as a condition to any recovery. This release will require you to reimburse DWS for any amount of a loss covered by DWS that is later recovered by you through other means. DWS may modify or withdraw the Account Security Program at any time.

All funds involve a certain degree of risk. Some funds have more risk than others. Please read the fund's prospectus before you invest or send money. War, terrorism, sanctions, economic uncertainty, trade disputes, public health crises and related geopolitical events have led and, in the future, may lead to increased market volatility and may have significant disruptions in U.S. and world economies and markets, which may lead to increased market volatility and may have significant adverse effects on the fund and its investments.

Obtain a prospectus

To obtain a summary prospectus, if available, or a prospectus, download one from www.dws.com, talk to your financial representative or call (800) 728-3337. We advise you to carefully consider the product's objectives, risks, charges and expenses before investing. The summary prospectus and prospectus contain this and other important information about the investment product. Please read the prospectus carefully before you invest.

The brand DWS represents DWS Group GmbH & Co. KGaA and any of its subsidiaries such as DWS Distributors, Inc. which offers investment products or DWS Investment Management Americas, Inc. and RREEF America L.L.C. which offer advisory services.

Investment products: No bank guarantee | Not FDIC insured | May lose value

DWS Distributors, Inc.
222 South Riverside Plaza Chicago, IL 60606-5808 www.dws.com
service@dws.com
Tel (800) 621-1148