**Email:** Reauthorize Accounts for **Open Banking Migration
From:** Platform Provider or Advisor
**To:** Investor

Subject: Action Required: Reauthorize Your Financial Account Connections

Hello <<first name>>,

We’re upgrading our systems to embrace the benefits of “Open Banking”—a more secure way to give your advisor access to your financial data.

Our account aggregation partner, ByAllAccounts, recently completed a migration for <<Financial Institution Name>>. This migration will require you to reauthorize access to the data leveraging the new open banking connection.

**IMPORTANT: To provide you with accurate reporting, it is critical that you complete the reauthorization steps as soon as possible.**

The new process will direct you to your financial institution’s site for authentication, creating a safer and more transparent experience for you. The process is simple and secure and can be completed in just a few simple steps.

**Please Note: For your security, we never ask for your credentials via email. To reauthenticate, please:**

[Provider to Add Full Instructions Based on User Experience]

1. Visit our official website <<Add Name>> or open our official app
2. Log In
3. Go to Your Account Linking Dashboard
4. Click “Connect” to Re-Link Your Accounts for <<Financial Institution Name>> & Follow Prompts
5. Confirm Accounts Have Linked

Here is a link to a guide [add hyperlink] or video [add hyperlink] that helps walk you through the detailed reauthentication process.

Please let me know if you have any questions about reauthorizing your broken account connections.

Best Regards,

<<Name>>

<< Email Signature>>

Tips to Make Sure This Does Not Look Like a Phishing Attempt:

1. **Use Official Email Addresses**: Send the email from an official email address that customers are familiar with and can verify.
2. **Brand Consistency**: Ensure the email design is consistent with your brand's official communications, including logos, colors, and fonts.
3. **Clear Language**: Use clear and straightforward language to explain why the reauthentication is necessary.
4. **Provide Instructions**: Give detailed, step-by-step instructions on how to reauthenticate, possibly with a link to an official guide on your website.
5. **Avoid Direct Links**: Do not include direct links to the login page. Instead, instruct customers to visit the website by typing the URL themselves or through their usual method, such as via the official app.
6. **Contact Information**: Provide a way for customers to contact your customer service team directly if they have concerns.
7. **Information on Phishing**: Briefly educate them on how to recognize official communications from your company versus phishing attempts.