Payroll Fraud Prevention

What are the Benefits of Maintaining a Separate Payroll Account?

- A separate Payroll Account is used only for payroll transactions. This separates ordinary payroll transactions from your main operating account activity, which makes it much easier to reconcile and to file quarterly wage, salary, and tax information.
- When your employees cash their payroll checks, only your Payroll Account number is exposed rather than having all of your account balances at risk.
- You should maintain an account balance that meets or slightly exceeds your payroll amount. This will allow you to identify fraud or errors quickly and easily should they occur.
- In the event of fraud, it is oftentimes much easier to quickly close the Payroll Account since there are fewer transactions and lower balances than a main operating account.
- You can limit check-writing and Online Banking access only to employees who are responsible for that function.
- If you are using a Third-Party Service Provider, you can place a debit filter on your Payroll Account to allow ACH transactions only from this Third-Party entity and for a maximum dollar amount.

Be Aware of the Payroll Diversion Scam

Cyber-criminals are focusing on employee payroll accounts via a payroll diversion scam. Phishing emails are designed to capture employee login credentials by appearing to be from an email address similar to a legitimate company. Once the employee's credentials are received, the cyber-criminal will use the credentials to logon to the employee's payroll account and change the bank account information. This change could prevent the employee from receiving any future alerts regarding changes to their direct deposit. The direct deposit can then be re-routed to an account controlled by the cyber-criminal.

In addition, cyber-criminals are also targeting Third-Party Service Providers. An email is generated from what appears to be from a company that does business with the Third-Party Service Provider. The email requests that new employees be added, or existing payroll amount and account information be changed. This can also result in direct deposits being routed or re-routed to an account controlled by the cyber-criminal.

How Do I Protect My Business Against Payroll Fraud?

- If a request to change bank account information is received through email, follow-up with the employee in person or by telephone before taking action. If by telephone, be sure to use a number already on file to verify that the request is legitimate.
- If you are using a Third-Party Service Provider for your payroll processing, implement a security program that is unique to your company. This should always include a telephone call to an authorized representative when the Third-Party Service Provider receives an email from your company requesting to change employee(s) information.
- If you are using a Third-Party Service Provider for your payroll processing, ask if there are controls in place to protect against fraud and describe what those controls are.
- Monitor employee log-ins that occur outside of normal business hours.
- Ensure that employee login credentials for payroll purposes differ from login credentials used for other purposes.
- Utilize multi-factor authentication for access to all systems containing sensitive information, including payroll information.
- Do not provide employees with login credentials or personally identifiable information via email.
- Review and update measures taken to protect employees' sensitive information and data.

How Do I Protect My Employees Against Payroll Fraud?

- First and foremost, alert and educate yourself and your employees of potential payroll scams.
- Instruct employees to hover their cursor over hyperlinks included in emails received to view the actual URL. This will ensure that the URL is associated with the company it appears to have come from.
- Instruct employees to refrain from supplying login credentials or personally identifying information through email or in response to any email.
- Direct employees to forward any suspicious requests for personal information to your firm's Information Technology and/or Human Resources Department.

800-442-6666
northwaybank.com
Member FDIC

Northway
BANK

The right bank makes a real difference