

Tompkins Fraud Prevention Tools

Our fraud prevention tools are designed to help you quickly identify and mitigate fraudulent activity.

Positive Pay with Payee Match

Our highest level of check fraud mitigation

Positive Pay with Payee Match is a fraud mitigation service that enables you to review and authorize checks and ACH debits paying against your account. When items are presented for payment, our matching and validation process quickly identifies checks and ACH debits that are inconsistent with the issued check file and ACH debit information you provide. We then notify you of any exceptions for you to review and decide whether to pay or return each item by noon.

Reverse Positive Pay

We provide you a daily exception list of all checks and ACH debits presented for payment from your account. You review the items and decide whether to pay or return each item by noon.

Positive Pay

We'll compare the information on issued checks and ACH debits to that of your issued check file and ACH debit information you provide. We then notify you of any exceptions for you to review and decide whether to pay or return each item by noon. Positive Pay will not identify altered payees.¹

Positive Pay with Payee Match	Highest level of protection, signature product. Business will provide bank with issued checks file. Business will be responsible for reviewing all exceptions and executing pay/return decision. Business adds payee name to issue file as an additional point of comparison.	Level of Protection: High Customer Involvement: File upload required, manual review of all exception items.
Reverse Positive Pay	Business is responsible for reviewing all check and ACH transactions and executing pay/return decision.	Level of Protection: High Customer Involvement: Daily Review of paid items (no uploading required).
Positive Pay¹	Business will provide bank with check issued information; Business will be responsible for reviewing all exceptions and executing pay/ return decision.	Level of Protection: Medium Customer Involvement: File upload required and daily manual payee verification by business through digital banking.
Daily Review & Reporting Process via Digital Banking²	Business will log on to Business Digital Banking to review prior days' payments. Business must review all transactions and check images from the prior day and timely notify the bank of any unauthorized payments.	Level of Protection: High Customer Involvement: Daily manual review of each check image posted in digital banking account to verify payee and amount on each item.

If you do not wish to enroll in one of our Positive Pay fraud mitigation tools, you must review the prior business day's transactions through our Business Digital Banking and notify us of unauthorized payments at no additional cost.

Each morning at 7:00 a.m., images of checks that have posted to your account the prior evening and ACH debits will appear in your Business Digital Banking profile.

If you rely on this as your fraud mitigation tool, you must review these transactions each business day prior to 11:00 a.m., and report any fraudulent items from the Posting Date to our Customer Care Center at 888-273-3210 before 11:00 a.m. Eastern Time on the Review Date.

Service Fees apply to Positive Pay services. ¹ Positive Pay without payee-match will not detect altered payee information. If your business uses Positive Pay without payee-match to detect fraudulent items, please also verify payee names using a Daily Review & Reporting Process (described above). ² If your business uses digital banking to detect fraudulent items, please log onto your Business Digital Banking account each business day (the "Review Date") prior to 11:00 a.m. Eastern Time to review images of checks that posted to your account(s) the prior day (the "Posting Date") and report any fraudulent items from the Posting Date to our Care Center (888-273-3210) before 11:00 a.m. Eastern Time on the Review Date. This option requires high customer involvement, as your business is responsible for reviewing transactions occurring on the Posting Date each morning, identifying potential fraudulent activity and then timely notifying the bank of any unauthorized activity. If you do not implement and properly use one of the methods described above to timely detect fraudulent activity, we will not be responsible for fraudulent transfers and will not be required to re-credit your account.

Fees subject to change.
Visit tompkinsbank.com/fraud-protection for additional information.