BOND SCHOENECK & KING

MEMORANDUM

TO: Kimberly Richards,
Warren County Attorney

FROM: [redacted]

DATE: June 16, 2026

RE: Phishing Scheme: Conclusions and Recommendations [redacted]

Executive Summary

Warren County was defrauded in late 2025 through a phishing scheme that caused approximately $1.34 million in net losses after partial recovery. Fraud actors impersonated a County vendor and successfully redirected legitimate vendor payments.

The incident resulted from systemic failures, including lack of vendor verification procedures, a public-facing ACH authorization process without safeguards, and unclear departmental responsibility for payment changes.

The fraud was preventable and not attributable to any single error, but to gaps in process, oversight, and training.

To reduce future risk, the County should strengthen internal controls by centralizing payment change authority, requiring independent verification of vendor requests, tightening ACH and wire controls, enhancing employee training, formalizing fraud alert procedures, and requiring vendors to promptly report known fraud schemes.

Background

On January 15, 2026, the Warren County Board of Supervisors engaged Bond Schoeneck & King, PLLC ("Bond") to (i) conduct an investigation regarding a fraudulent phishing scheme that targeted the County and (ii) to provide legal advice and recommendations to the County Attorney based on that investigation.

I conducted this investigation in cooperation with FAZ Forensics ("FAZ"), which the County separately retained to examine the phishing scheme but also other financial issues that went beyond Bond's scope of work.

With FAZ, I conducted interviews of: (i) County Auditor Carla Sherman, (ii) Senior Account Clerk Claudia Mundell, (iii) DPW Superintendent Kevin Hajos, (iv) Deputy Treasurer Monica Stark, (v) Accountant Dan Donohue, (vi), Treasurer Christine Norton,

[redacted]

(vii) Senior Programmer Analyst Jeremy Scrime, and (viii) County Administrator John Taflan. We sought to interview two former employees, Rob Lynch and Ellen Rose, but each declined.

Summary of the Facts

Creation of ACH Authorization Process for Vendors. On November 26, 2024, then-Deputy Treasurer Rob Lynch asked Warren County IT (specifically, Jeremy Scrime) to create a fillable Automated Clearing House ("ACH")[1] authorization request form that would be accessible via the Treasurer's Office main web page. IT fulfilled this request the following day, on November 27, 2024, creating a form that could be accessed and filled out by anyone who clicked on "Vendor ACH Authorization Form" on the Treasurer's web page, as follows:



TREASURER

Services
Certificate of Residency
Short Term Rentals Occupancy Tax
Occupancy Tax Information and Forms
Educational information on short-term rentals
Warren County Tax System
Forms
2025 Petition & Notice for Foreclosure
Vendor ACH Authorization Form

Reports
Financial Reports
Budget Reports

Treasurer

The Treasurer's Office is responsible for administering the financial affairs of Warren County. The continuing objectives of this office are to improve financial accounting and reporting systems; to provide improved services to County departments and State and Federal agencies; to improve services to the public.

Statement From The Treasurer

The Warren County Treasurer's Office is responsible for administering the fiscal affairs of the County. Our staff is dedicated to our citizens and strives to provide the public and our agencies alike with the highest level of professionalism. Through a wide range of services including the collection and disbursement of funds, this office is able to aid its customers while monitoring and reporting the County's fiscal health.

Under my Administration, the philosophy of the Treasurer's Office will continue to be one of safeguarding the taxpayer's monies and implementing cost effective strategies whenever and wherever possible. I welcome ideas and input from the public and look forward to improving the financial outlook for Warren County.

CONTACT INFORMATION

Warren County Treasurer

Christine Norton, County Treasurer

Phone: (518) 761-6375
Fax: (518) 761-6470

Email County Treasurer

Hours
Mon- Fri, 8:30am - 4:30pm

Deputy Treasurer Lynch declined to be interviewed for this investigation; his request on November 26, 2024, was consistent with Treasurer Norton's stated goal of making ACH available as a payment option to vendors. No vendor utilized the "Vendor ACH Authorization Form" feature until May 2025.

On May 20, 2025, when the Treasurer's Office received its first ACH payment request from a legitimate vendor using the web form, Deputy Treasurer Lynch notified some of his colleagues in the Treasurer's Office and said, "we will need to come up with

[1] An ACH payment is an electronic transfer of money between bank accounts that is processed through the Automated Clearing House (ACH) network, a U.S. system used by banks and financial institutions to move funds in batches.

[redacted]

some written procedures on how this needs to be handled." (Treasurer Norton was not included on this email.)

Peckham Fraud Alert. Peckham Industries ("Peckham"), based in Brewster, New York, is a vendor for the County Department of Public Works ("DPW"), as well as for some Towns within the County. Peckham is one of DPW's largest vendors (if not the largest). In July 2025, Peckham sent a notice to its business partners labeled "Fraud Alert: Impersonation Attempts Targeting Our Business Partners." Two County DPW employees received the alert, as did the offices of Towns with which Peckham has worked (e.g. Town of Queensbury, Town of Warrensburg). The alert stated in part as follows:

> We are reaching out to inform you of a matter that requires your immediate attention. We have been made aware of recent fraudulent activity where fraudsters are impersonating our company and members to deceive customers and redirect payments.

The alert further advised, "We have not changed our banking information. Any request to alter payment instructions should be treated as suspicious unless independently verified. ... Verify any request to change banking details by contacting your regular representative via a known phone number." To the extent anyone read and understood this alert, they did not share it with the County offices that play a role in making payments, e.g. the Treasurer's Office and Auditor's Office.

At a meeting on October 23, 2025, the County Attorney's Office advised the Treasurer's Office, including Treasurer Norton and Deputy Treasurer Stark, that the Treasurer's Office lacked the authority to sign contracts to conduct wire and ACH transactions absent Board of Supervisors approval. The County Attorney's advice did not cause the Treasurer's Office to change its processes, particularly since the Treasurer's Office had been using ACH for years to make non-vendor payments (e.g. payroll).

On or about the following dates, Warren County DPW received legitimate invoices from Peckham in the following amounts:

October 21, 2025	$546,784.27
October 21, 2025	$1,065,121.31
November 4, 2025	$520,574.65
November 12, 2025	$1,005,646.59
November 13, 2025	$220,308.06

All of these invoices specified that Peckham be paid by mailed check; dating back to 2020, all Peckham invoices were paid by paper check with the exception of one small payment conducted via credit card.

[redacted]

Phishing Scheme. Between November 10, 2025, and December 8, 2025, one or more people, believed to be the perpetrators of the fraudulent scheme, placed calls to County Departments on 16 different occasions. Of these 16 attempts, 10 of these phone calls were answered with 9 of the answered calls taking place within the Treasurer's Office. The timeframe of the 9 phone calls within the Treasurer's Office ranged from less than 1 minute to approximately 8 minutes in duration.

On November 12, 2025, a man spoke with Claudia Mundell in the Treasurer's Office. During this conversation, Ms. Mundell likely inadvertently disclosed pertinent information regarding Peckham accounts. Ms. Mundell did not do anything to verify that the caller was from Peckham.

On November 13, 2025, Ellen Rose in the Treasurer's Office received a phone call from a man with an Indian accent. The man identified himself as a representative from Peckham and inquired about payment of an invoice in a specific amount which Ms. Rose could not remember, but which was in the area of $2.1 million. Ms. Rose said she located an invoice, from Peckham, in the exact amount the man had mentioned.[2] The man asked about changing payment methods from paper checks to ACH payments. Ms. Rose directed the man to the "Vendor ACH Authorization Form" on the Treasurer's web page, and instructed him to submit an ACH authorization request form. Ms. Rose said she told the man that he needed DPW's authorization to change payment methods. Ms. Rose notified County Auditor Carla Sherman of Peckham's request; Ms. Sherman assumed that DPW had been in touch with Peckham.

On November 13, 2025, at 10:45 a.m., an online ACH authorization form was submitted to the Treasurer's Office. This form listed a company named Peckham Road Corp. (which is a subsidiary of Peckham Industries), a contact name of Rafael Diaz, a contact phone number of (347) 272-9617, and a contact email address of rdiaz@peckhhamroadcorp.com. This form requested that ACH payments be made to a Discover Bank account and listed a bank routing number for Discover Bank and an account number. No one in the Treasurer's Office verified that this was a legitimate request from Peckham. No one attempted to contact "Mr. Diaz" at the phone number and email address provided.

On November 15, 2025, the Treasurer's Office advised the Auditor's Office of this ACH authorization request. The Auditor's Office then advised DPW of this request and told DPW to place all of Peckham's invoices into a separate "batch" for ACH payment in lieu of paper check disbursement. No one consulted DPW about an apparent payment change request coming from one of its largest vendors.

---

[2] Ms. Rose declined to be interviewed for this investigation, and referred me to her written statements to Sheriff's Office and Comptroller investigators. I have reviewed her statement to the Sheriff's Office; from that review it is unclear how Ms. Rose could have located a Peckham invoice in the range of $2.1 million because, as set forth above, no single Peckham invoice was close to that amount.

[redacted]

In December, Ms. Rose in the Treasurer's Office received two listings for Peckham marked as ACH payments. Ms. Rose took these listings, went into the New World system and selected them as ACH payments and sent them to Deputy Treasurer Monica Stark for her review. Deputy Treasurer Stark approved the payment change to ACH. Ms. Rose then uploaded the ACH payment instructions to Arrow Bank.

On December 12, 2025, an ACH payment in the amount of $2,132,480.23 went from a Warren County account at Arrow Bank to the Discover Bank account listed on the ACH authorization form. This amount represented the total of the October 21 and November 4 invoices issued by Peckham.

During this time period, ACH payments were subject to a "cap," or daily limit, of $2 million. Due to this transaction exceeding the cap, an Arrow Bank representative contacted Deputy Treasurer Stark to obtain authorization to exceed the "cap" and to confirm the transaction. Ms. Stark approved the transaction.[3]

On December 23, 2025, a second ACH payment, this time in the amount of $1,225,954.65, went from a Warren County account at Arrow Bank to the Discover Bank account listed on the ACH authorization form. This amount represented the total of the November 12 and 13 invoices issued by Peckham.

Someone from Arrow Bank called Deputy Treasurer Stark about this second ACH transaction, and she approved it.[4]

Discovery of Phishing Scheme and Financial Impact. On December 23, 2025, Peckham contacted DPW about payments not received. This kicked off communications and investigation leading to the realization that the ACH authorization request was fraudulent, no one named Rafael Diaz worked for Peckham, and Warren County had been defrauded. On December 23, 2025, Deputy Treasurer Stark contacted Arrow Bank in an attempt to stop and reverse the second ACH transaction in the amount of $1,225,954.65. This transaction was still in a "pending" state and Arrow Bank was able to stop the transaction prior to any funds being dispersed.

Shortly after discovery of the fraud, County IT took down the "Vendor ACH Authorization Form" on the Treasurer's web page.

---

[3] There is a dispute over whether anyone from Arrow Bank told Deputy Treasurer Stark – in this call or a second, subsequent call – that this transaction was suspected to be fraudulent. Deputy Treasurer Stark was adamant that she was not informed about any possible fraud prior to approving this transaction. Arrow Bank appears to have not recorded its calls with Deputy Treasurer Stark, but has advised the Sheriff's Office that in a call with Deputy Treasurer Stark it raised the possibility of fraud.

[4] There is also an unresolved dispute as to whether anyone from Arrow Bank told Deputy Treasurer Stark that this second transaction was suspected to be fraudulent. Deputy Treasurer Stark was adamant that she was not informed about any possible fraud prior to approving this transaction. Arrow Bank has advised the Sheriff's Office that in a call with Deputy Treasurer Stark it raised the possibility of fraud.

[redacted]

The current loss amount from the fraud is $1,342,498.52, following insurance payouts in the amount of Two Hundred Fifty Thousand Dollars ($250,000) from Tokio Marine for cyber crime coverage and One Hundred Thousand Dollars ($100,000) from Travelers Insurance for crime coverage, and law enforcement seizures totaling $439,981.71 from three bank accounts that received fraud proceeds.

Conclusions

1. **This fraud, successfully perpetrated on the County, was the result of a "perfect storm" of poor decision-making**. The success of this phishing scheme depended on a combination of a number of things gone wrong, e.g. no vendor verification protocol, a public-facing ACH request form with no controls, and lack of interdepartmental communication. There were a number of junctures at which the fraud would have likely been prevented had one or more County employees exercised the appropriate level of diligence and care. My recommendations in the next section, therefore, are narrowly tailored to stopping a similar fraud from happening again and meant to add common-sense layers of extra protection.

2. **The decision to make ACH widely available, as a method for paying vendors, was not, and has never been, adequately justified**. Treasurer Norton cited the following as justifying the use of ACH to pay vendors: some vendors have asked for it, it is a faster method of payment, and it avoids check fraud. (By check fraud, Treasurer Norton seemed to be referring to instances in which a legitimately issued County check is altered to change the payment amount and payee, allowing the check to be deposited into an account designated by the fraudster.)

But only a handful of vendors have asked for ACH payment, and only 2-3 legitimate vendors used the "Vendor ACH Authorization Form" on the Treasurer's web page during the thirteen (13) months it was available. ACH is a faster method of payment than payment by check, but speed also creates risk in the event of an erroneous payment. Treasurer Norton did not identify any significant check fraud that has materially impacted the County's finances. Warren County also uses Positive Pay for its checking accounts[5], which greatly reduces the likelihood of check fraud; and even if check fraud occurs, the bank, not the County, typically bears the loss.

3. **The Treasurer's Office involved itself in vendor payment change requests without an adequate basis for being involved or adequate procedures**. Even if ACH were justified as a method of paying vendors, the Treasurer's Office was not the most logical place for changing payment method on a vendor-by-vendor basis, as it is not the office that regularly deals with vendors. The County Purchasing Department manages the County's vendor relationships. The changes requested by the

[5] "With Check Positive Pay, we compare a daily file with data on issued checks against checks coming in for payment on your account. We'll flag any exceptions for you to review via Business Online Banking, allowing you to decide if they are paid or returned." Arrow Bank, https://www.arrowbank.com/business/positive-pay.

[redacted]

fraudster should have been routed to the Purchasing Department for review and approval. There has been no adequate explanation as to how and why the Treasurer's Office involved itself in this matter.

The Treasurer's Office also lacked adequate procedures for changing payment methods. On the Tuesday before Thanksgiving 2024, Deputy Treasurer Lynch asked IT to place the "Vendor ACH Authorization Form" on the Treasurer's web page; the form was "live" and publicly accessible the following day. Yet six (6) months later, on May 20, 2025, Lynch wrote to some employees under his supervision, "we will need to come up with some written procedures on how this needs to be handled." The decision to have a public-facing ACH authorization form, and then to not put in place any protocols for handling such forms, is inexplicable. There also seems to have been no recognition that making this form publicly accessible, and allowing anyone to fill it out in the name of any vendor, created a significant risk of fraud. Also, the "Vendor ACH Authorization Form," when it was filled out, was not automatically routed to the County Purchasing Department that actually manages vendor relationships, which could have been a layer of protection against fraudulent submissions.

By November-December 2025, when the fraud occurred, the Treasurer's Office still had no protocols in place for receiving ACH instructions from vendors using the Treasurer's Office online form and processing ACH transactions in response to those vendor requests. The Treasurer's Office also lacked procedures for limiting its disclosure of financial information over the phone when dealing with members of the public, in accordance with the County's Red Flags Identity Theft Prevention Policy, Resolution No. 485 of 2024.

4. **The County lacked procedures for handling fraud alerts such as the one received from Peckham in July 2025, but the Peckham fraud alert urged precautions that the Treasurer's Office should have had in place regardless.** Peckham's fraud alert went unheeded because there were no procedures within the County for handling such alerts. Although the alert provided clear guidance – e.g. "Any request to alter payment instructions should be treated as suspicious unless independently verified" – no one who received or read the alert would have known how to act on that guidance due to the lack of County procedures for handling such alerts.

In any event, the Peckham fraud alert urged precautions that any County department handling payment method change requests – e.g. the Treasurer's Office – should have had in place anyway. These included treating as suspicious "[a]ny request to alter payment instructions ... unless independently verified" and "[v]erify[ing] any request to change banking details by contacting your regular representative via a known phone number." These are precautions that the County should have had in place regardless of whether a vendor had alerted it to a phishing scheme.

5. **County officials and employees lacked proper authorization to conduct ACH and wire transactions, but this lack of authorization did not contribute to the fraudulent scheme.** Over time, several County departments entered into banking agreements with Arrow Bank (and its predecessor, Glens Falls National

[redacted] Bank & Trust Company) without authorization from the Board of Supervisors, including a Wire Transfer Agreement signed on May 18, 2023, and an ACH Originator Agreement signed on February 29, 2024. In October 2025, the County Attorney's Office advised the Treasurer's Office that it lacked authority to execute such agreements absent Board approval.

However, this issue did not contribute to the fraud at issue. The scheme succeeded due to deficiencies in vendor verification, internal controls, and payment processing procedures – not the existence of ACH or wire capabilities themselves. Moreover, the record does not reflect that the Treasurer's Office was directed to suspend ACH or wire activity, and doing so would have significantly and unnecessarily disrupted routine County operations, including payroll processing.

Recommendations

1. **Put the Purchasing Department in charge of vendor payment method change requests.** This was already accomplished via Resolution No. 118 of 2026.

2. **Place limitations on ACH and wire payments to vendors.** ACH is not in high demand among vendors. The County Purchasing Department, which is now responsible for vetting payment method change requests, should require that any request for payment by ACH or wire be justified by the vendor's own circumstances rather than making ACH and wire payments available to any vendor that makes a verified request. Payment by check should continue to be the principal method of paying vendors. The reason to require a vendor to provide specific justification for switching to payment by ACH or wire is that a fraudster would have a harder time articulating a credible reason for making a switch.

Changes already made by the County – e.g. creation and implementation of the "New Vendor Request Form/Vendor Change Form," and obtaining baseline data from every vendor that can be used to verify future requests – are also warranted, but requiring a vendor to provide a specific reason for switching payment methods adds yet another layer of protection against phishing schemes.

The County should also require a mandatory waiting period (e.g. 5 to 10 business days) between approval of a vendor payment method change and issuance of the first payment under the new method. Fraud schemes usually rely on urgency – a waiting period tends to kill that advantage (although it did not do so in this case).

3. **Lower the ACH "cap" at Arrow Bank and require additional approval of any transactions exceeding the cap.** The current daily limit for ACH is $2 million. The County should lower the cap to $500,000, to better align with the current maximum insurance payout (per incident) on the County's cyber crime policy, $250,000. (The County has already reduced the wire cap from $9 million to $500,000, to better align with its insurance coverage.)

[redacted]

Additionally, for the purpose of adding an extra layer of protection, Arrow Bank should be instructed to seek and obtain the approval of the County Finance Committee Chairperson for any ACH or wire transaction above the $500,000 cap. Based on FAZ Forensics' analysis of the County's banking activity in 2025[6], I estimate that requiring County Finance Committee Chairperson approval of ACH and wire transactions above $500,000 would result in Arrow Bank calling the County Finance Committee Chairperson approximately 2 to 3 times per month – a manageable number of calls.

4. **Mandatory, in-person training on phishing schemes**. The County should mandate in-person training – and real consequences for failing to complete training – for any employee who (i) has access to non-public financial information and (ii) has occasion to communicate with members of the public. Such training should cover, at minimum, common phishing schemes, means of properly verifying who someone is, and the limited types of information that can be communicated to a member of the public, in accordance with the County's Red Flags Identity Theft Prevention Policy. Employees should also be occasionally tested with simulated fraud scenarios to reinforce training and identify gaps.

5. **Require vendors to agree to enhanced fraud notification obligations**. The County's standard vendor contracts should require a vendor, upon becoming aware of any impersonation, payment redirection attempt, or other fraud scheme touching on its organization, to promptly notify the County by (i) email to and (ii) direct telephone contact with the County department administering the contract, with an email copy to the Purchasing Department and County Attorney's Office. To the extent commercially feasible and subject to negotiation, vendor contracts should also include a provision allocating responsibility for losses that are directly attributable to a vendor's failure to provide timely notice of a known fraud risk, including appropriate indemnification mechanisms consistent with applicable law. These provisions are intended to ensure timely information sharing and to shift the risk and burden of any loss onto the vendor.

6. **Implement a red-flag system for any vendor fraud alerts that the County receives.** Ideally, a fraud alert could be entered into the County's New World system and then become a "red flag" whenever a payment to this vendor is in the process of being made. The County employee processing the payment would then be required to resolve the red flag before completing payment processing.

[6] ACH transactions above $500,000 in 2025: 21
Wire transactions above $500,000 in 2025: 14