1. Meeting Minutes
   Documents:
   
   FINANCE COMMITTEE. 01-22-20 PDF

2. Agenda
   Documents:
   
   1-22-2020 FINANCE AGENDA.PDF
Theodore Roosevelt Building
1550 Franklin Avenue
Mineola, New York

January 22, 2020
3:10 P.M.
APPARENCES:

LEGISLATOR HOWARD KOPEL
   Chair

LEGISLATOR VINCENT MUSCARELLA
   Vice Chair

LEGISLATOR TOM MCKEVITT

LEGISLATOR ROSE MARIE WALKER

LEGISLATOR ELLEN BIRNBAUM
   Ranking member

LEGISLATOR CARRIE SOLAGES

LEGISLATOR SEILA BYNOE
LEGISLATOR KOPEL: We are going to start. I'm going to take the roll. Then I will make a short opening statement. Then we will get going here. Start with the pledge.

Thank you everyone. Mr. McKevitt.

LEGISLATOR MCKEVITT: Here.

LEGISLATOR KOPEL: Ms. Walker.

LEGISLATOR WALKER: Here.

LEGISLATOR KOPEL: Ms. Birnbaum.

LEGISLATOR BIRNBAUM: Here.

LEGISLATOR KOPEL: Substituting for Mr. Drucker would be Ms. Bynoe.

LEGISLATOR BYNOE: Here.

LEGISLATOR KOPEL: And substituting for Mr. Lafazan would be Mr. Solages. I'm informed that Mr. Muscarella is on his way down. We have a quorum. So we can go ahead at this point.

Earlier this month the comptroller held a press conference at which it was announced that 700 some odd thousand dollars in taxpayer dollars had been sent from his office to a fraudulent entity. As we understand it we don't have a lot of details.
Finance 1-22-18

on this. This occurred some time in late October of 2018. We basically don't know anything about it here. At least I don't. 2019, excuse me. Takes me a while to adjust to the year. By October or so I should get it right.

We basically know about it from Newsday.

Mr. Schnirman, thank you for being here today. We appreciate your coming down here to enlighten us as to what happened and to answer our questions. Because it's our job, it's your job to ensure that the office of comptroller has all the necessary procedures and controls in place so that tax dollars are not inadvertently sent to third parties that are not entitled to this money.

Now, this was reported in the press as a cyber attack. But we've got a lot of questions understandably. So what we want to do is find out what exactly went wrong over here in the process which enabled this money to be sent to the wrong party. What procedures there were in place prior to this
occurrence. What, if any, procedures have been implemented since then to prevent a recurrence. We look forward to hearing the answers to these questions and more to protect the Nassau County taxpayers' hard earned money.

Just a word as to how we are going to conduct this hearing. Mr. Schnirman, why don't you come and sit in the hot seat right here please. I believe Mr. Schnirman has an opening statement if I'm not mistaken; is that correct?

MR. SCHNIRMAN: We do.

LEGISLATOR KOPEL: Mr. Schnirman and whoever is with him will present the opening statement. At that point the Majority and Minority members of the committee will ask questions. After that we're going to allow other members of the legislature who are in attendance today but are not members of the committee we're going to let them ask questions as well if they are so inclined. And finally, of course this is a hearing, we're going to allow questions and comments
Finance 1-22-18

from the public. With that, Mr. Schnirman, the floor is yours.

MR. SCHNIRMAN: Good afternoon.

I want to thank the Finance Committee of the legislature for holding today's public hearing and for inviting us to speak on the financial and payment security and controls within the office of the county comptroller. I'm here today because modernization of the county's financial system is a concern that my office has proactively looked at since day one. The critical component of that issue is cyber security.

As technology improves and advances at a rapid pace, malicious actors have weaponized that technology and are using it to attack governments, private industry as well as private citizens. Increasingly cyber attacks have targeted municipalities throughout the country costing taxpayers and residents millions of dollars.

A report released last fall said that in the previous ten months 140 local governments, police stations and hospitals
Finance 1-22-18

have been held hostage by ransomware attacks. Just recently it was announced that a ransomware attack hit Albany International Airport. We've also seen this right here in Nassau County with school districts targeted in Rockville Centre, Lynbrook and Mineola.

As cyber attackers adapt the threat only worsens. It's incumbent upon all of us to ensure that we undertake necessary and critical efforts to modernize our financial system so we can remain vigilant against the threat of cyber attacks and further protect taxpayer dollars.

To be clear, the incident that was reported to the police was not a cyber attack on the county's overall IT infrastructure. This was a focused and elaborate phishing scheme that used a vendor's correct tax ID number. Used a modified check to falsely change a vendor's bank information to divert funds. The claims for payment were normal and regular. In the scam we are here to discuss the destination of the payments is what was fraudulently altered. In the end all the
monies were recovered and the county's books are even.

Recently I joined Police Commissioner Pat Ryder to announce that there was an attempted cyber attack on Nassau County, as well as the full recovery of more than $700,000 in county funds that were initially diverted to bank accounts due to this elaborate but ultimately unsuccessful scam.

Controls in place at the time, which have since been enhanced, identified this fraudulent activity and the account that the money was diverted to was frozen. As a result of a coordinated investigation, which included the Financial Crimes Detectives Unit of the county police department, the Office of the County Treasurer, Nassau County District Attorney's Office and the Nassau County Comptroller's Office, all monies were recovered. The cyber attackers were thwarted in their attempt to scam the county. The county lost no monies. The vendor received payment and additional controls were put in
Finance 1-22-18

place that will further deter similar future scams.

Procedures in place and implemented by our office's Claims Division ensured that county funds are protected. The team in the Claims Division not only audited and approved over 65,000 claims to thousands of vendors in 2019, but increased oversight and efficiency in the process saving taxpayer dollars.

Since we took office in 2018 our claims division has identified several millions dollars in erroneous or duplicative claims ultimately saving the county money. An example of this success is in the catching of the American Water bill that had increased from $45 per month to approximately $4,500.

Gabe Marques is here, our fiscal office from the Claims Division and we thank our division for their hard work.

But let's all remember, no matter how vigilantly we prepare vulnerability to cyber attacks is a problem. We've improved our controls. We did this before this incident. We have now improved our controls
after this incident. But even as our defenses increase, attackers will continue to attempt to work around them. So we know we must continue to work to improve because even we are all vigilant we are all still vulnerable.

So let's get right into it. Deputy Comptroller and chief counsel Jeff Schoen and fiscal officer Gabe Marques are prepared to give an account of the attempted scam as well as the protocols that have since been implemented to further protect county funds against future attempts.

To give a brief overview, our team implemented new controls when we first came into office because there was no consist method to verify vendor information. We looked thoughtfully and updated the controls to make the process more centralized, more efficient and increase oversight.

A number of changes were implemented from January of '18 to August of '19. This is a result of identifying the importance of accurate vendor information in the digital age and we will look to continue
Finance 1-22-18

to make updates as we go.

To update the vendor information form we required enhanced verification, including a cancelled check and verifying tax ID numbers. Since this incident we have enhanced controls further. These now include an enhanced vendor information form. Enhanced verification and confirmation of vendor information provided. Internal comptroller's office trainings are now ongoing and have been ongoing. There's also been a countywide IT training on how to identifying phishing attempts. And in looking forward, the electronic vendor portal adds additional comprehensive levels of security by requiring a log in and a password to submit a vendor information form.

And today I am pleased to announce that these new controls have stopped at least one subsequent attempt in which a real vendor was targeted in the same way using a mimicked email address. In December of 2019 a claims auditor received a request to change banking information for a vendor. Due to the new
internal controls the request was flagged. The scammer was unable to provide the newly
required enhanced verification and vendor information. In working with the vendor, the
scam was identified and the fraud was stopped by the Vendor Claims Division of the
comptroller's office.

I'm going to turn it over for a moment to deputy comptroller and chief counsel
Jeff Schoen to walk us through a power point with the specifics.

MR. SCHOEN: As to the specific phishing attempt, the comptroller's office received an email from a scammer disguised as
a county vendor requesting to modify the vendor's automatic bank payment information or
ACH payment. The scammer sent the request from an email address which mimicked that of
an actual email address of the principal of one of the county vendors. For example, the
actual email address being jprincipal at ABC incorporated dot com but instead mimicked that
with a dot net. As we all know, scammers are mimicking email addresses all the time. We
Finance 1-22-18

all receive them on our phones and devices on
a daily basis.

The fiscal officer informed the
scammer that they must complete a new vendor
profile form.

MR. MARQUES: Good afternoon. So

as a process of the controls, we asked the
scammer to fill out a new vendor information
form, which was returned completed with the
correct tax identification number, the correct
vendor name, the correct vendor contact name,
which was an authored principal of the
company, the correct vendor address and a
correct vendor phone number. In addition, a
voided check was submitted, as you can see on
this slide, that had the accurate vendor name,
the accurate vendor address and an actual bank
account number at Chase Bank was submitted.
Those two documents were submitted in
conjunction and then forwarded on for
processing.

MR. SCHOEN: So this was a

mimicked real check.

Subsequently, the comptroller's
Finance 1-22-18

office was informed that a bank account receiving county payments had been frozen. This indicated possible fraudulent activity. The comptroller's office identified 710,000 plus in payments to this account. The comptroller's office initiated a joint investigation with the Nassau County Police Department, the county treasurer and the district attorney's office and all payments were recovered.

So how did we get here? Before a vendor can be paid a vendor must submit a payment information form to the county. Typically done on an IRS form W-9. What's called a request for taxpayer identification and certification. The county's W-9 form is known as a 700 form.

Prior to January 1, 2018 there was no centralization of the process of collecting this form. There was no consistent method to collect or verify the vendor information. And most importantly, the comptroller's office was not verifying that the tax identification numbers, the TIN numbers, businesses social
Finance 1-22-18

security number essentially, was not verifying that those were in fact actually TIN numbers. Between January 2018 and August 2019 our office centralized the collection of vendor information in the comptroller's office. We centralized and uniformed the method of verification of vendor information in the comptroller's office to the Vendor Claims Division. This included the verification of the banking account information requiring the void check or requiring a letter from the bank saying that this is in fact the vendor's bank account. And utilizing a free service that the IRS provided of verifying that the TIN numbers, the social security numbers of the vendor, were in fact actually numbers. And if that failed, we would essentially deactivate the vendor and not allow the financial systems to make any payments to the vendor until those problems were resolved.

After the event, the phishing event, we enhanced the vendor information form. We required that the vendor tell us if
they were submitting a new form or they were making changes to the form. And specifically to check what changes they were making to that form. More importantly, we asked them to provide their old banking information, both the bank, the routing number and the account number and the new one. Because if you were attempting to mimic as if you were an old vendor and you were in fact someone phishing and trying to defraud us, most likely you wouldn't know the old information. You would only know the new information.

We also put in enhanced verification and confirmation of the vendor information. Are you actually making this change? Asking multiple checks with more than one person with the vendor. Contacting more than one person. One person asked to make the change and another person verifying the change. We also did a training at the comptroller's office as well as the countywide training that IT implemented.

On top of that, all that, very soon, we will be requiring the vendor
Finance 1-22-18

information form to be submitted through the vendor portal. The vendor portal, as we all know, requires log in and password access from the vendor in order to access it. So if you were a vendor who wants to submit a form you're going to have to be an authorized user of the vendor's profile in order to get in another. On top of all these extra controls we put in place, there will now be a log in and access controls in order to submit the vendor information form through the vendor portal.

As the comptroller pointed out, these internal additional controls have already thwarted a similar attempt.

MR. SCHNIRMAN: So simply put, this scam was about using a mimicked email address on the vendor information form. Currently our antiquated financial system, which was developed prior to the regular use of corporate or personal email addresses, cannot accept email address information in the vendor profile screens. New financial system will be able to electronically verify email
Finance 1-22-18

addresses and therefore will be able to
identify a situation with a mimicked email
address and this underscores the need for
modernizing the county's finances that we've
talked about before. And for that reason I
again thank the legislature for supporting the
financial modernizations that are now moving
forward.

The announcement of the phishing
attempt was held with law enforcement
following the full recovery of the diverted
funds so as not to interfere with an active
investigation and in the interest of providing
full transparency and accountability to the
public. As Commissioner Ryder said, money
moves quickly and this scheme was not
exclusive to Nassau County. In fact, three to
four other municipalities were also targeted
we were told. We needed to recover the money
before the scammers could be alerted and move
the money. But the key thing is that working
with investigators we recovered the county's
money and zero dollars were lost. All efforts
to be transparent have served as a positive.
Since the announcement, representatives from other municipalities, even from other parts of the country, have reached out in the interest of preventing similar schemes from occurring in the areas that they represent. And this healthy dialogue must continue. Just this morning I joined Suffolk County Executive Steve Bellone to discuss partnering on cyber security on a regional basis. But this is not a Nassau problem or even a regional problem. This is a challenge that all governments, municipalities, businesses and private citizens face as we are more dependent on technology to manage our day-to-day life. So we look forward to working together.

I want to thank again the legislature again for supporting the financial modernizations that are moving forward. Nassau County must take the lead in modernizing our government and ensuring that we are fully prepared to protect tax dollars now and into the future no matter the threat.

We are looking to partner with
other municipalities on cyber initiatives as we go forward. In fact, months before this incident, the comptroller proactively took up the issue of cyber security with its revitalized independent audit advisory committee. The issue was discussed actually in April of '19 and June of '19 a specialist from the county's external auditor gave a detailed presentation on cyber security. And in September of '19 the committee once again received an update on the issue.

In fact, this year technology was built into our recent procurement of external auditors. As a sign of our concern for cyber security, our new external auditors have dedicated personnel for the integration of technology assessment services which includes cyber security. These auditors have already met with the county's IT department to discuss this critical issue.

So before we take any questions that you have, I want to again thank the committee for taking a thoughtful approach to this issue and sincerely hope that we can
partner on initiatives to promote good
government to protect taxpayers, the county
and critical modernizations as we go forward.

I will caution that while we have
gotten into quite a bit of information about
the incident here, as our counsel will remind
me I'm sure, we are reticent to get into a
certain level of granular detail as that would
be unsafe I would say to our public safety
going forward. With that, we are happy to
take any questions the committee may have.

LEGISLATOR KOPEL: Thank you for
your presentation. I just want to note for
the record that Legislator Muscarella joined
us at the outset of this presentation and he
is now with us and in full attendance.

Let me ask you a few questions.
I'm not quite clear on several details on the
actual attack here. We will call it an attack
for convenience. First of all, how many
payments were made comprising this entire
710,000?

MR. SCHNIRMAN: I want to give
you a general answer and then I'll let Deputy
Finance 1-22-18

Comptroller Schoen give you -- as I said earlier, and I can see how this can be a point of confusion, this was not an attack on the county's overall IT infrastructure.

LEGISLATOR KOPEL: We understand that. I'm not really -- don't want to get hung up on terminology at this point. I called it an attack. We will call it whatever you would like. What would you like?

MR. SCHNIRMAN: Absolutely an attack. It's just that there's a different piece, right, whether it's the overall IT infrastructure or this was --

LEGISLATOR KOPEL: I said during this attack. I did not refer to the IT infrastructure at all. I merely referred to this incident as an attack and I will continue to if that works for you.

MR. SCHNIRMAN: Sure.

LEGISLATOR KOPEL: How many payments?

MR. SCHOEN: The information that I provided in the presentation is what we are comfortable to say publicly. In interest of
Finance 1-22-18

public safety we would have to give you

anymore details in executive session.

LEGISLATOR KOPEL: Was there more

than one?

MR. SCHOEN: After being notified

that the payments were going into a fraudulent

account we identified other payments going to

that account. That's the 710,000 is a

composite of multiple payments.

LEGISLATOR KOPEL: Understood.

That does answer the question. How did this

come to light? We did not really get into a

good level of detail. How did you find out

that this is a problem?

MR. SCHOEN: We were notified by

our banking institution that the payments were

attempting to go into a fraudulent account.

LEGISLATOR KOPEL: When did this

happen?

MR. SCHOEN: The notification was

in late October.

LEGISLATOR KOPEL: When were the

payments being made more or less?

MR. SCHOEN: That's not a level
Finance 1-22-18

of detail we're not prepared to give outside
of executive session.

LEGISLATOR KOPEL: Is it safe to
say that it was some months prior to that?

MR. SCHOEN: It was a less than
30 day period of time.

LEGISLATOR KOPEL: Now, I'd like
to go into some of the -- let me ask you
this. Did you notify the administration?

MR. SCHOEN: We immediately
notified and put together the investigative
team of the county treasurer's office and the
police department which are under the
administration's purview.

LEGISLATOR KOPEL: Did you notify
the county executive's office back in October
or thereabouts?

MR. SCHOEN: As I said, we worked
with the police department and the treasurer's
office which are under the county executive.

LEGISLATOR KOPEL: So no, you
didn't notify the county executive? That's a
no?

MR. SCHOEN: Yes. Yes, we did.
MR. SCHNIRMAN: Yes, we were in contact with the county executive's office at that time.

LEGISLATOR KOPEL: That's what I asked you. Would have been simple to just say yes or no.

Getting into the procedures. You've gone through a lot of these procedures as to how information is provided to the county and you've got it all in writing and you've got all kinds of information there. Are you aware that there are certain best practices common to the industry? When I say industry I should say industry in general not the industry. I don't mean only the county's. But pertaining to anyone that gets involved in making large wire or electronic transactions and it's out there on the Internet. You can find dozens of instances of it very simply. You're aware of that, are you not?

MR. SCHOEN: Yes. We've tried to implement a lot of practices that weren't in place including the requirement of the
cancelled check, the requirements of the bank letter and now the additional verifications, the dual verification of an individual requesting a change and verifying with the company that the change is in fact being made.

LEGISLATOR KOPEL: Are you aware that a change in payment instructions is a classic red flag, are you not?

MR. SCHOEN: We receive hundreds of requests to change payment instructions. We receive both new vendors and vendors that already exist with us to make changes. We get about 30 or so requests per week. Over 1500 requests per year.

LEGISLATOR KOPEL: Your procedure in dealing with that is to change the paperwork essentially? In other words, you've gone through these --

MR. SCHOEN: Currently the financial system requires us to do it on paper. We are going to be shortly going to the vendor portal where it will be submitted electronically with the enhanced control of the log in and password in order to do that.
LEGISLATOR KOPEL: It seems to me that using not only the prior controls but even the current controls, a disgruntled insider is still in a perfect position to game the system. A disgruntled insider, he or she would have access to all the information you need.

MR. SCHOEN: I think that would be the case in any institution. But I believe --

LEGISLATOR KOPEL: So that's correct?

MR. SCHOEN: If we went into executive session we would be able to give you the additional controls we put in place.

LEGISLATOR KOPEL: I'm speaking quite generally speaking. It seems to me that these particular controls could easily be gained by any, as I say, disgruntled insider. Let me ask you, are you not aware that the best practice for change of any kind of wire instructions from those given at the very outset of a transaction generally requires verification by a phone call.
emanating from the payor to a known person and
a known phone number at the payee?

MR. SCHOEN: Exactly what we're
doing now. That's one of the controls that I
would like to talk about in executive session
so as not to inform the people scamming us as
to what our processes are.

LEGISLATOR KOPEL: That's not a
big secret as I say. That is a universal best
practice. So we weren't doing that?

MR. SCHOEN: We were not and we
are now.

LEGISLATOR KOPEL: And are all
emails encrypted?

MR. SCHOEN: You have to ask IT.

It's an IT question.

LEGISLATOR KOPEL: It sure is an
IT question but it's also a question for you
because that's something that again it's a
best practice when you're dealing with any
kind of transaction details. I'm not an IT
person but I know that I'm in business and if
I need something I'll go to IT and say hey,
best practice is here's the list, have you
Finance 1-22-18

implemented it? And if you haven't you better do it for us real quick. Did you ever ask them for that? I'm sorry, did you answer?

MR. MARQUES: Us at the claims division we rely on IT to provide that level of security. The truth of the matter is that it's a largely manual process and any time you have a manual process risk is inherent.

LEGISLATOR KOPEL: So you haven't? The answer is no, not yet?

MR. SCHOEN: I'm not sure at what point we decided to look into it but right now the financial system does not even take an email address or cannot take an email address. The email addresses are used at the claims division to communicate with vendors. And the vendor information form will be coming through the vendor portal which requires an email log in and password access.

LEGISLATOR KOPEL: Going into some other best practices. When you make payments how is that handled? Explain that to us.

MR. SCHOEN: The comptroller's
Finance 1-22-18

office actually doesn't make payments. The comptroller's office approves payments and then all those approved payments are put on what we call a warrant which is sent to the treasurer's office. The treasurer's office actually makes payments. That's the control in place. The comptroller's office in fact can't make payments. That's the nature of control in place in the county charter.

Treasurer pays comptroller approves.

LEGISLATOR KOPEL: Good. Is there just one person to doing those approvals?

MR. SCHOEN: We have various levels of approval depending on the amount of the payment. But all of the individuals in our claims division have approval level depending on the level of the claim.

LEGISLATOR KOPEL: But it's a single person?

MR. SCHOEN: There are multiple claims auditors who can approve payments. Depending on the amount of the payment there may be additional levels of approval required.
LEGISLATOR KOPEL: In a given instance, if there was a significant amount of money there would be more than one person looking at this?

MR. SCHOEN: Yes. Even before it comes to our office it would have been reviewed by the department and then sent to us for approval.

LEGISLATOR KOPEL: The other question, I guess you probably won't know the answer to that, when somebody does get into the system do you require multifactor authentication? It sounds to me like that's something that you are starting to do.

MR. SCHOEN: Yes. With the vendor portal. IT will be able to answer that more specifically.

LEGISLATOR KOPEL: It sounds to me like that's something you're starting to implement but haven't yet. But we will save that for IT I guess. Tell us about the training programs that you've implemented here.

MR. SCHOEN: Apart from the
Finance 1-22-18

countywide IT training which all received I believe due to the phishing incident. We have been monitoring other incidents in other -- that happened and regularly advising our claims auditors what to look for based upon those instances.

LEGISLATOR KOPEL: I'm talking specifically about the people in the comptroller's office who are responsible for authorizing payments. We've already established I think that you are about or have just about implemented the program where you would be calling to verify transactions.

MR. SCHOEN: We haven't but since October, since the incident, we put that in place.

LEGISLATOR KOPEL: What happens? Which kind of payments will require phone calls for? All payments?

MR. SCHOEN: Yes. What happens is the payments are separate from the payment process. A vendor receives payments based upon a claim that's been approved. The vendor sets that profile up before they can get any
payments using the vendor information form. That form is where they set up their payments. How they're going to get paid. If they want to make any changes they use the vendor information form to make changes.

The initial form and any changes to that form we are doing that dual verification. So one person from the vendor will request the change and we will verify with someone else at the vendor, preferably the contact person on the contract, we will verify by phone that they in fact are making the change. And then we have an additional control which we send them an email, which we all get when we make changes to our accounts, that says hey, you made a change to your account. If this didn't happen please let us know.

LEGISLATOR KOPEL: Please let us know again it's not sufficient. You have to have these phone calls.

MR. SCHOEN: Absolutely.

LEGISLATOR KOPEL: It's old tech

but --
MR. SCHOEN:  It's amazing how new tech requires the old tech.

LEGISLATOR KOPEL:  And fax machines. Fax machines are back in use for wire instructions. I would advise you not to take wire instructions on email at all. Not only not to verify it don't take them. Get it by fax or get it verbally. That's again it's a best practice. Unless sometimes a backup would be an encrypted email. But you probably don't have that.

What kind of information -- you implemented some time ago your open checkbook program?

MR. SCHNIRMAN:  Correct.

LEGISLATOR KOPEL:  Question that I have for you is, how much information is available as a result of this program that can be used by some of these evildoers?

MR. SCHNIRMAN:  We implemented a transparency portal Open Nassau dot Nassau County NY dot gov. On there is Open Checkbook, Open Budget, Open Payroll. Our score card as well. Looking at the county's
finances. So simply put, the information that is there is the same information that was previously publicly available but it's displayed in a more user-friendly fashion. Previously it was put up in just Excel sheets. Sort of hard for the average individual to wade through.

LEGISLATOR KOPEL: But is any of this information information that might have made it easier in this particular incident and possible others?

MR. SCHNIRMAN: The information was already available.

LEGISLATOR KOPEL: I'm sorry. I don't understand.

MR. SCHOEN: The platform we're using is a different platform. But all the information was already available. And it was already made publicly available and would be completely have to be made available under the New York State FOIL laws.

LEGISLATOR KOPEL: Not information. Not bad checks and so forth.

MR. SCHOEN: Yes.
LEGISLATOR KOPEL: Information about checks?

MR. SCHOEN: You can check with your counsel but --

LEGISLATOR KOPEL: I'm not contradicting you.

Now, your office found out about this because you were notified by a bank that happened to notice irregular activity on this particular account to which the money went. I think that's what you said, right?

MR. SCHOEN: Correct. We always rely on our financial institutions to help protect fraudulent activity on our credit cards and banking.

LEGISLATOR KOPEL: This is very unusual and lucky because the great majority of times I understand that this money within minutes is out of the country. So I'm sorry this was a crook who didn't know his or her business very well I guess. So it's really just pure dumb luck that we got this money back.

MR. SCHOEN: The fact that we
Finance 1-22-18

reacted as quickly as we did once we were informed, the fact that we keep electronic records so we were able to identify the accounts as quickly as we did and the fact that the department --

LEGISLATOR KOPEL: I'm saying it happens within minutes. Literally minutes. It usually happens money goes into an account it's gone within minutes.

MR. SCHOEN: I think they're able to move it from the initial account to different accounts but it's very hard to get the money out of those accounts. It takes a more sophisticated process to actually get the money in your hands and these investigations, as was announced, was able to identify other accounts that it went to.

LEGISLATOR KOPEL: I understand but typically, as I say, money comes in, you have preexisting instructions and that money comes into an account and it's immediately wired to Bulgaria or God knows where. Then it's gone.

MR. SCHOEN: Then you have to get
the money out of that account in some way.

LEGISLATOR KOPEL: It's wired to Bulgaria or something as I say. I picked on Bulgaria. I don't know why.

MR. SCHNIRMAN: The police commissioner went into this at some length, and I know that there are representatives from the police department who can probably speak to that as well.

LEGISLATOR KOPEL: We found out only because this was caught by the bank. Now there is some delay between the time that an invoice is rendered and payment is made. That's typical. There's a delay of I don't know whether it's 30 or 60 or 90 days. I don't know what that is and that's not really my question. My question is, what assurances do we have that there's not a couple of other time bombs sitting in your file that we don't know about yet?

MR. SCHOEN: After the incident we reviewed six months worth of vendor information request changes and verified all the changes.
LEGISLATOR KOPEL: You're satisfied that there's nothing else out there at the moment?

MR. SCHNIRMAN: To the best of our knowledge yes. But as I mentioned earlier and I think it's important to remember, we will continue to update our controls just as others are in other places. Yet we are all still going to be vulnerable. So just as scammers will continue to improve we have to continue to improve. That's what we are committed to doing.

LEGISLATOR KOPEL: You are hereby requested to give the committee members, and if it's in confidential form that's okay too, but we would like a full current exposition of what all your current controls are. And you might as well identify those that have been updated as a result of this incident and perhaps as a result of this discussion.

With that I'm going to turn it over to Legislator Muscarella and then Legislator McKevitt.

LEGISLATOR MUSCARELLA: Hi. I'm
kind of ignorant of this stuff. I'm not a
computer guy. I know how to use one. So I'm
not into all the terminology and I'm not into
all of the sophistication. Let me ask you a
couple of just basic things. You indicated
the phishing attempt and that the scammer got
the following information. Correct tax ID
number, vendor name, contract name, address
and phone number. Any idea where they got
this information?

MR. SCHOEN: No.

LEGISLATOR MUSCARELLA: So there
was a phishing expedition by the scammer. Did
somebody do a forensic evaluation of your
computer as to where this information might
have come from?

MR. SCHOEN: I think you may be
getting into details of the investigation that
the police department could tell you about.

LEGISLATOR MUSCARELLA: So let me
ask you. Basically, the computers are being
looked at, correct? As part of the
investigation now.

MR. SCHOEN: The manner in which
they perpetrated the phishing scheme is being investigated as part of how they were able to identify, from my understanding, how they would be able to identify the bank account.

LEGISLATOR MUSCARELLA: Let me give you my basic concern. That this was less a phishing scheme and more a fraud perpetrated on the county. And I'd like to know in executive session maybe whether or not the information that was acquired by the scammer was general information that was gotten very easily by a member of the public or was gotten as part of the electronic phishing scheme.

Number one.

Because if it was general information that's out there, then that information should no longer be put out to the general public because it's information that is being used by someone against us.

Number two, I just find it incomprehensible that when someone asks us to change the direction of where money is going that the comptroller's office asks for a check for the new account and has never thought to
Finance 1-22-18

ask for information verifying the old account. It appears to me that the comptroller's office found out about this not by any inquiry by the comptroller's office, not by any hit that IT might have found that there was something going on with our computers, but solely, fortuitously, by a bank that notified us that we were being hacked or phished or whatever.

Maybe this is unfair, but we constantly get audits by the comptroller's office, every department, everything, and invariably just about every department that the comptroller's office does an audit on comes back with the common theme you have inadequate safeguards. Inadequate safeguards for timekeeping, for paying bills, for accounts, receivables accounts payable. All kinds of inadequate safeguards. Yet it appears to me that we're the victim of our own inadequate safeguards in the county. I understand all the controls that we are having from this point forward.

Comptroller, you indicated that
there were similar inquiries made from other places that are being subject to similar type scams. Were any of those successful that you know or were they just --

MR. SCHNIRMAN: To our knowledge yes.

LEGISLATOR MUSCARELLA: Just as a matter of course, I would hope that you're aware of the legislation that the legislature passed and went into effect that requires notification of the county legislature in the event you are subject of a hack or phishing scheme or that kind of thing and I just note that there was no such notification done here.

MR. SCHOEN: Just to that specific piece of legislation. It requires the county IT department to notify the legislature and other people within 72 hours of a breach or cyber attack on the Nassau County's information technology infrastructure. On the core of the structure.

LEGISLATOR MUSCARELLA: So what you're saying is it doesn't fall technically
within the purview of that legislation and in any event it's not your responsibility to do it, it's IT's responsibility.

MR. SCHOEN: According to this piece of legislation.

LEGISLATOR MUSCARELLA: So then perhaps we'll have to change the legislation.

MR. SCHNIRMAN: To be clear and it's what we talked about at the beginning, this was not an attack on the overall county IT infrastructure. It was a different kind of situation.

LEGISLATOR MUSCARELLA: I have no other questions right now.

LEGISLATOR MCKEVITT: My understanding is that the way that this legislature found out about this incident, I believe it was a press conference that was held on January 11th of this year. Would be would that be correct I believe?

MR. SCHNIRMAN: I believe so.

LEGISLATOR MCKEVITT: At that press conference I believe you, Mr. Schnirman, indicated that there were controls in place
Finance 1-22-18

immediately identified this fraudulent activity and the account that the money was diverted to was frozen. I believe that would be an accurate summarization of what you stated at that press conference. Would that be correct?

MR. SCHNIRMAN: Yes.

LEGISLATOR MCKEVITT: But the controls in place were not controls of the county comptroller's office. They were actually the controls of the bank where the money was being sent to. Isn't that the case?

MR. SCHNIRMAN: No, actually as our chief counsel had said. That is one of our controls.

MR. SCHOEN: We rely upon the banking institutions that we all have to tell us when things -- there's a fraudulent activity on the account that we have that we are involved with them.

LEGISLATOR MCKEVITT: But as far as controls, is that a protocol on what type of suspicious activity to be looking for come
from your office or is that just something that the banking institution does in general with all their banking customers?

MR. SCHOEN: I guess the answer to both of those questions would be yes.

LEGISLATOR MCKEVITT: So this you believe is actually the protocol the bank has just for its institutions in general not necessarily something specific to Nassau County finances and accounts, would that be correct?

MR. SCHOEN: Correct.

LEGISLATOR MCKEVITT: Just a little bit of concern too, I know one initiative which has been happening in the last couple of years is the Open Checkbook website in order to be able to go and give more transparency to the public. My concern is I'm just on Open Checkbook right now and literally I can see checks for as little as $4, literally see checks in greater amounts like that. And my concern is yes, we definitely want to be transparent with the public how the money is being spent, but in
other instances can this just be a game plan showing a prospective fraudster or scamster as to at least identifying who the vendors are so they can actually find this information and go down this route.

MR. SCHNIRMAN: I think we spoke to that earlier but I will let counsel.

MR. SCHOEN: I think both this legislative body and other legislative bodies, and the main legislative body in the state has unfortunately told us given this multiple instructions on how to put information out to the public and how to protect public information. The information that is out there is all information that would be required to be made public.

LEGISLATOR MCKEVITT: I guess again that's part of the dilemma. Yes, we want to be transparent as possible but just again by looking on this website I can easily tell you with probably within a Google search within 30 seconds I can tell you the names, the phone numbers, probably the CEO. Probably the only thing I could not easily get is
taxpayer identification number. That's the one I probably could not get as easily on this website.

MR. SCHOEN: I think you're right. There are competing interests there. The people of the state have required that our legislature pass laws that require us to put information out there in a transparent way and that's what we do. It's unfortunate that it could be utilized for nefarious purposes. But that's the line we are riding. We're trying to abide by the law and be as transparent as possible. We have competing statutes.

LEGISLATOR MCKEVITT: Thank you.

LEGISLATOR WALKER: I just have a very quick question. When you said the email address was mimicked. So perhaps at the end instead of saying dot com it says dot net. As soon as anything was different about that that didn't draw attention? Didn't give you some thought in your mind why is this different?

MR. MARQUES: Without being specific in public about the actual change,
Finance 1-22-18

one step is that at the time the name of the individual was listed in our book rather than the actual address.

But second is that up until a few months ago the vendor portal, which is what we are using right now as the official record of vendors, did not exist. So we did not know what the official email address of the vendor was.

MR. SCHOEN: In the financial system currently there's no place to put an email address into the vendor profile in the financial system. It did not take it. It doesn't understand what an email address is because of the age of the financial system.

LEGISLATOR WALKER: For the comptroller. When you started your statement you said this was not a cyber attack. However, throughout part of your discussion you called it a cyber attack. So it was, it wasn't. To me it's some type of cyber attack. I'm not too good on this either. I'm lucky that I can do whatever you are supposed to on the computer. I have no way I can
figure out how to do something that you shouldn't be doing.

MR. SCHNIRMAN: I appreciate the question and the opportunity for clarification. To be clear, it absolutely it was a cyber attack. What I was saying is, it was not a cyber attack on the county's overall infrastructure. It was a specific targeted phishing scheme not meant to infiltrate the overall cyber infrastructure of the county. But meant to phish a particular payment to get that. Hopefully that's a little clearer.

MR. SCHOEN: Generally cyber attacks fall in these two categories. One being the phishing category and the other being the more attack on your infrastructure, ransomware type category. This was more the phishing category. But they are both categorized generally as cyber attacks.

LEGISLATOR WALKER: So now when you were notified by the banking institution did you try to do any investigation yourself or did you immediately reach out to the police department and to the county executive and to
Finance 1-22-18

the DA's office?

MR. SCHOEN: We immediately look
at our electronic records to see what the
payments that were going to the account and we
identified the payments and then notified the
police department and the treasurer and began
the investigation.

LEGISLATOR WALKER: I will pass
for now.

LEGISLATOR BIRNBAUM: Thank you
for clarifying a lot of what I don't think we
had heard about before. My question is
regarding the amount of funds. In this case
approximately 710,000. If this had been a
lesser amount, let's say a much smaller amount
in total, do you think that the banking
institute would have noticed? Was it because
of where the location of the account had been
changed to? The distance? Was it the amount
of the payments? What flagged it?

MR. SCHOEN: The account itself
had already been flagged as a fraudulent
account. There's probably a lot of money
going into that account. So it wouldn't have
mattered whether we were trying to put a penny
in there or whether we were trying to put
multiple thousands of dollars.

LEGISLATOR BIRNBAUM: In other
words, the scammer was using this account for
other scams as well?

MR. SCHOEN: Yes. There were
other municipalities on Long Island that were
scammed in the same way.

LEGISLATOR BIRNBAUM: By the same
person or individual, whatever.

MR. SCHNIRMAN: In addition I had
just add, in the more recent attempt that we
mentioned earlier that was thwarted back in
December, the amount of money at stake was a
significantly smaller amount of money and our
enhanced controls now caught that.

MR. SCHOEN: That's just based
upon the amount of business we do with that
vendor.

LEGISLATOR BIRNBAUM: So then
leading up to what Legislator Kopel said, if
it had been a more sophisticated scammer that
wasn't doing an account across the country and
Finance 1-22-18

was trying to transfer it to say another
country, do you think that it might not have
been flagged as easily?

    MR. SCHOEN: You can probably
talk to law enforcement more about this. The
Financial Crimes Division may know more about
this. Essentially the scammers like this they
attempt to get money into accounts they have
control over and then move the money into
other accounts they have control over. But
going the money out of the account is really
the sophisticated part. It's somewhat easier
to get it there but you have to somehow get it
out. You need multiple resources to take that
money out. If you take money out in big
amounts it's going to be flagged.

    Not to get into what the criminals
do, I don't know myself, but you need multiple
resources and a real system in place in order
to actually get control of the money. You
have to get it out and utilize the money.
That never happened. In this case that never
happened.

    LEGISLATOR BIRNBAUM: The account
Finance 1-22-18

that was it going into was that person even aware that was happening?

MR. SCHOEN: To our knowledge no. As Commissioner Ryder stated, it was a woman on the west coast who didn't even know this account was being utilized.

LEGISLATOR BIRNBAUM: Did the vendor notice that the payments were not being made on a timely basis?

MR. SCHOEN: No because the time period of the payments was less than our 30 day payment period. Although sometimes our payments are more than 30 days. But it was certainly within our normal payment period. So they were not expecting those payments necessarily. They would have been shortly but they weren't expecting them at the time.

LEGISLATOR BIRNBAUM: Now you're feeling fairly confident that with the portal setup, with everything going through emails it will be --

MR. SCHOEN: The portal is an ultimate layer of control in effect. So you can't submit it unless you're a vendor who has
access. We still have all the other controls behind it. The phone calls that Legislator Kopel talked about. The verification by phone call and the other layers of protection that we have added in order to make sure that we don't make any changes until everything is completely verified.

MR. SCHNIRMAN: I would add, as we said the good news here is that the county's made whole. The county's not out any money and controls continue to improve. And as we talked about the technology that we are using is improving and we have planned improvements coming up as well. But I think we have to just be really open about the fact that this was yesterday's scam. Right? And as we talk about moving forward I think we have to anticipate that the sophistication will continue to improve and so must our efforts continue to improve and on and on we go.

LEGISLATOR BIRNBAUM: In a way this was like a wake up call. It really got the county to start implementing procedures
Finance 1-22-18

that should may have been in place but I'm really glad we are moving forward and it will be --

MR. SCHOEN: Since this administration got here we were looking at the importance of these payments and how they were made and looking at those enhanced controls that we started to put in place in January of '18 and progressed to where we are now.

Starting with verifying the TIN numbers, which was never done. Asking for the cancelled check or the bank note. As Legislator Kopel pointed out is a common thing to do. We were even doing that. We centralized in our office. So the departments aren't verifying vendor information in different ways. We're verifying it all in our office. We are allowing the vendors to submit the information directly to our office and doing the review in our office. We've taken ownership of it and we continue to enhance the controls as electronic information gets more susceptible.

LEGISLATOR BIRNBAUM: Just to go over one more time about Open Checkbook. This
site is simply organizing information that had already been available to the public on our website but in a different format?

MR. SCHOEN: Yes. I would argue that the public requires us to put out to them in a transparent way.

LEGISLATOR BIRNBAUM: Is Open Checkbook actually what other municipalities use?

MR. SCHNIRMAN: Yes. There's a variety of them. Also the Town of North Hempstead has one. New York State. Around the region and the country this is the direction that governments are going in terms of transparency.

LEGISLATOR BIRNBAUM: Thank you very much.

LEGISLATOR BYNOE: Good afternoon. So, are you seeing any correlation between municipalities having these breaches and the efforts to make information more transparent?

MR. SCHNIRMAN: No.

LEGISLATOR BYNOE: You're not
Finance 1-22-18

seeing any correlation between the two?

MR. SCHNIRMAN: I don't think that we have seen.

LEGISLATOR BYNOE: I'm hearing a lot more often than I'd like that a school district has been in some way targeted and then we're hearing that not only did we have one vendor but you said later on there was a second vendor, there was an attempt. I was just wondering, maybe this is a question for law enforcement and not your office.

MR. SCHNIRMAN: I think perhaps.

LEGISLATOR BYNOE: I'll leave that question alone then.

MR. SCHNIRMAN: But I would just mention just locally we have seen attacks in Rockville Centre, in terms of school districts, Rockville Centre, Lynbrook, Mineola on the school district side.

LEGISLATOR BYNOE: Yes, I'm aware. That's what led me to ask the question.

So, you mentioned that you would manually now send an email to each entity
which you have said is somewhere around 30
terities per week, which is about 1500
terities, vendors per year that are making
changes to their account. So you're going to
make the change using your newly established
verification procedures. Then you're going to
do what? Manually send them an email to say
we've made this change to your account. If
you have not requested this change please
notify us?

MR. SCHOEN: Right. That's the
only way to do it now. The financial system
cannot handle the email. There may be ways to
automate it but right now we are doing it
manually. The individual who makes the change
who is already verified by phone or email by
somebody else at the vendor that they are in
fact making the change will then send an email
as sort of a final precaution to say hey, we
made this change. If you didn't authorize it
let us know.

LEGISLATOR BYNOE: Because a
member of senior staff suggested then it made
me think about how I'm communicated with by my
Finance 1-22-18

bank and by others that I receive a wire. US Department of Housing when they send the wire they just don't rely on me waiting to get notification from my bank. They also send me a separate email that says we wired you XYZ dollar amounts for this purpose, for this program area and it's broken down. Then there's a grand total as to what should have been wired into my account.

MR. SCHOEN: That would be very easy to do if we had a modern financial system. We can certainly look into a process to do something like that with our current limitations.

LEGISLATOR BYNOE: To notify a vendor that a payment had been made.

MR. SCHOEN: Right.

LEGISLATOR BYNOE: So you're saying right now there's no way to do that?

MR. SCHOEN: We could look into the possibility of doing it. But I could tell you for sure that it could be done when we modernize our financial system.

LEGISLATOR BYNOE: Where are we
Finance 1-22-18

in modernizing our system?

MR. SCHNIRMAN: So, first of all, thank you to the legislature on a bipartisan basis of appropriating funds to move that process forward. The HR system is looking forward to come online in the near future and we are in the preimplementation phase with the overall ERP system.

LEGISLATOR BYNOE: Can you be more specific?

MR. SCHOEN: We are currently in the process of reviewing proposals from a vendor who will provide preimplementation services helping us to determine what the exact services need to be provided for a new system. What the system should look like and what the RFP for the new system should look like. We are looking for a vendor to assist us in the preimplementation phase.

LEGISLATOR BYNOE: We will partner with law enforcement as well to make sure that the system is going to have all of the different capabilities to reduce our risk?
MR. SCHOEN: As part of why we are looking for a preimplementation vendor is to help us develop the controls against cyber attacks for whatever new system.

LEGISLATOR BYNOE: So we don't think law enforcement is a natural partner in helping us look at that process either?

MR. SCHOEN: They could be.

LEGISLATOR BYNOE: I think they should be. They're the ones facing this on a daily basis and they're communicating with their colleagues across the country.

MR. SCHNIRMAN: As we said earlier, when it comes to cyber security we're looking to broaden the partnerships and have that kind of dialogue.

LEGISLATOR BYNOE: So, there are a lot of payments to go out. I was also on Open Checkbook at the same time my colleague Legislator McKevitt was on. When I look at the volume that goes out there's a lot. There's a lot of payments. So, I didn't have enough time to peruse it but I would say any vendor that's getting multiple payments at
Finance 1-22-18

a sum of $710,000 in a one-month period we
should be hypervigilant in making sure that we
are looking at any changes to those types of
accounts. I'm not saying that -- any tax
dollar that is not appropriately protected
would be a shame on us. But I would think
those that are going out at higher volumes and
with higher risk we should be definitely
looking at those a lot closer.

MR. SCHOEN: Absolutely. That's
one of the additional levels of control that
the vendors with higher payments if they're
making any changes to their accounts need to
be reviewed at a higher level within the
Claims Division.

LEGISLATOR BYNOE: Very good
thank you for sharing that. Thank you.

.

LEGISLATOR SOLAGES: Comptroller,
again, thank you very much for your
presentation and thank you to your team. Just
also if we can send out an email or any
notification to our vendors where there's a
lot of transactions and asking them also to be
Finance 1-22-18

part of the process. Asking them that if
taxpayer ID on their part was somehow leaked
to please notify us of that as well. Because
that's something that was not under your
control. How this perpetrator was able to
secure and get that taxpayer ID information.
That's my only suggestion here and I thank you
for your presentation.

LEGISLATOR KOPEL: Before I turn
it over to the noncommittee members just
before that I have to say I'm sorry, I
apologize in advance but I'm disappointed that
you chose to put this into a press conference
and the comptroller's office took credit for
stopping a fraud when the information that
we've heard here today was nothing but pure
dumb luck that we got this done. If the money
would have gone into the hands of a more
competent fraudster this money would have been
gone and indeed it might be still continuing
today if not for that.

We are going to really want to very
closely see the new procedures and make a
determination in this committee as to whether
Finance 1-22-18

those are sufficient and as to whether we
ought to recommend some further action.

With that, I'm going to turn it
over to Legislator Ford.

LEGISLATOR FORD: Good afternoon
and thank you very much Chairman Kopel for
giving me this opportunity to also ask
questions. And I just want to start out by
saying Legislator Muscarella did bring up a
good point. As we have seen with your office
that you have audited many departments and
bringing out their inadequacies in regards to
their safeguarding and, you know, possible
leaks or any faults that may lie with them
especially dealing with any of the money that
we have. Any money that is within Nassau
County.

It seems that according to your
testimony here that you brought up the fact
that these phishing attempts and these cyber
attack attempts, and I guess I'm like
Legislator Muscarella and everyone else, I'm
not really very proficient with software and
IT and everything. But it seems that these
attacks can happen and they have been
happening. So much so -- and correct me if
I'm wrong on this -- that you had indicated in
April of '19, June '19 you brought I guess the
people in your department in for training in
regard to these type of IT safeguards or
whatever else can be done because of the
possibility of any type of attacks or any type
of fraudulent activity that can occur, am I
correct?

MR. SCHNIRMAN: What we had said
is in April and June of '19 cyber security was
something that we brought up with our
independent audit advisory committee and it's
something that we are working on in our
office. Incidentally, both the Majority and the
Minority in the legislature are represented on
the committee. We had discussion with our
independent auditors at that time about best
practices and ways to protect the county going
forward.

LEGISLATOR FORD: These
independent auditors did the discuss then at
that point that we can all of a sudden you
Finance 1-22-18

could have somebody who may try to scam money
out of the county? Did they talk about that
then? Because it seems, according to you,
that we're all aware. I think everybody we're
all aware. Even on our personal accounts we
all know that anybody can access -- I have to
be very careful with my passwords. I have to
be concerned about whether or not somebody's
going to steal a check or whatever. To take
all these safeguards. People can sign up with
Lifelock or anything to protect their identity
and also to protect any type of money that has
been fraudulently taken from them. But that's
my own thing.

You as a comptroller, you're
responsible for the safety of the county's
money. I just want to know when you had this
in April and June when you had these
discussions knowing full well that is
something that can happen. And as we know now
it did happen. And thankfully the bank caught
it. What did you indicate to the people that
worked for you to be aware of the fact that
something like this can happen?
Finance 1-22-18

MR. SCHNIRMAN: As we said earlier, we increase the controls immediately in 2018. We continue to increase them in 2019. It's something that we've been working on throughout 2019. And now we have increased them going forward as well and we have plans to continue to do so going forward.

LEGISLATOR FORD: When we look at this, when we look at this type of fraud that happened, how many people basically in your department were involved in this that were able to allow this account to get paid without anybody really checking? And did you ask --, you know, when I know that sometimes with contracts and any other type of submissions by anybody for payment for vouchers it goes through ten points of like checks. Did you ask to see whether or not those changes should have gone through other departments as well to see whether or not this was indeed a valid change?

MR. MARQUES: Let me start by just explaining how the changes operate as a function of administration. The comptroller's
claims decision we have two separate sections. One that handles the auditing of invoices. And one that handles the vendor information. So I think that clears up a lot of misconception about how payments and the vendor information are intermingled. There is a wall between the two.

The vendor information, the way it operates is a purely manual system. Someone is entering this information into a computer. That one individual, now we have two individuals processing this information. Also share other duties. And like the comptroller said, we process about 1500 changes. Some vendors have more than 30 different payment accounts. They're rather large. I would say the controls have changed. The last two years the controls have gotten much better than they were before.

I will say that more vendors contact our office about legitimate payments that they don't know what they're for than asking if a payment went to a wrong account. So, with that, I'm pretty confident that the
controls we did have in place were good and
now they're better given the limited system
that we have to work with. Basically fighting
a war with sticks and rocks.

LEGISLATOR FORD: So then when
you talk about -- you're saying that there's
actually two separate departments. So in
order for this vendor to have submitted this
check -- so the person who accepts the invoice
and clears the invoice or claims voucher,
there's a wall between that person and the
person actually making the payment?

MR. SCHOEN: For each claim
there's not a new claim -- payment
information. A vendor is set up with a
profile so that they can get paid. That
profile includes their various payment
information. Their bank account information
for ACH. If they want to get a check where
that check was to go to. The payments are
made based upon the vendor profile. The
payments get approved by the comptroller, go
to the treasurer to pay. The treasurer pays
based upon that vendor profile in the vendor
Finance 1-22-18

system. The vendor profile is entered in this manual process that the fiscal officer explained. Is entered by the hard workers of the claim division into the financial system.

LEGISLATOR FORD: So with the vendor profile -- then I'm a vendor. I say I want -- this is my account. This is who I am and whatever claims I have you're going to send to my account at TD Bank. Here I am. That's what you do.

Then all of a sudden I decide or somebody decides that it's going to be Denise Ford. But I said, you know, not so much TD Bank anymore. I want it to go to Chase. So nobody checks to make sure that, like, why all of a sudden she's changing her bank? And knowing full well that we can be subjected to fraudulent activity on the part of anybody just to get some money out of us.

MR. SCHOEN: The vendor is required to submit the updated form. That form, with all of the controls that we put in place since January '18 and the additional controls subsequent to this incident,
including the phone calls, the dual verifications and now or in the near future with the form being submitted to the vendor portal.

LEGISLATOR FORD: So then who did you call in regard to this bank? If you're saying that you had all these controls in place, that ever since 2018 you had these controls in place -- no, I'm listening. I hear what you're saying. You said that you have all this because if somebody is going to change a bank you're going to do your due diligence because you're handling everything manually. Then all of a sudden now somebody decides to change their bank. Who did you call to verify that that information was correct?

MR. SCHOEN: The control in place at the time, the major control in place at the time was the submittal of the void check. The phisher mimicked that check. That's why we put the additional controls on where one person from the vendor is asking for the change and then we're going to be contacting
another person at the vendor, preferably the contact on the contract, to verify that they are in fact making the change and verifying all the banking information with that individual.

LEGISLATOR FORD: So who did you call?

MR. SCHOEN: The control at the time was the void check. We have now the additional control of a phone call.

LEGISLATOR FORD: You said before that since 2018 you had these checks and balances in place.

MR. SCHOEN: No. I said we've been developing them since 2018. We had initial ones we put in place, the void check, checking the TIN and we've layered on the additional controls and, post the incident, we layered on the additional controls of the phone calls and the additional verifications.

LEGISLATOR FORD: So what you're testifying today about is everything that you've changed since this scam happened but we want to know what did you do beforehand? I do
Finance 1-22-18

have a problem with this.

MR. SCHOEN: Before we went from not verifying TIN numbers. Not asking for a cancelled check to verify the bank account number. We weren't doing any of that. We had decentralization where each department was verifying the information independently. So we centralized all that in our department. That was the developing of additional controls since January 2018.

LEGISLATOR FORD: You didn't go far enough. That's really what I'm looking at. If this could happen and if you're talking about trying to get an updated new security system. We're talking about hundreds of thousands, millions of dollars, millions of dollars of taxpayer money.

Now you reference that prior to 2018 it really was whatever. So do we know offhand, or maybe when we can go into executive session we can ask the police, how many scams occurred against the comptroller's office prior to January 2018 and how many fraudulent payments? When you talked about
like when the vendors call up and they say
that now they can question whether or not it's
a legitimate payment, what did you mean by
that?

MR. MARQUES: We do get a number
of inquiries into our office by vendors who
have submitted claims for work performance or
goods provided that do get paid on a timely
basis.

MR. SCHOEN: It's a restriction
of the financial system. So if you get paid
by a check, depending on your banking
institution, there may be a note on that check
that tells you exactly what invoice is being
paid or what isn't being paid. But there's a
restriction -- our current financials, our
antiquated financials system cannot in the ACH
payments, electronic payments, sort of tell
the vendor exactly why they're getting that
payment. The vendor needs to work with their
own banking institution or inquire directly to
us as to what that payment was for. That's
what Gabe was referring to was they often call
up and say I got this check from you guys, I
got this payment from you guys, what was that for? Could you correlate that back to the invoices that were in fact approved on the claim?

LEGISLATOR FORD: Is that still happening today?

MR. SCHOEN: It's a limitation in our financial system, yes.

LEGISLATOR FORD: So you're making no effort at this point so that like -- because then you can make a payment to somebody's account and if the person isn't going to go honest enough to say, you know -- if I got money in my account, like there are people that they get money in their account and they say wow, look at this look. It's like Christmas in July and I can spend this money. How do you know that some of the payments you made were not made incorrectly?

MR. SCHOEN: The claims themselves -- there are no fraudulent claims here. All the claims themselves are vetted and approved.

LEGISLATOR FORD: There was a
fraudulent claim. A couple of them.

MR. SCHOEN: No, there was not a fraudulent claim. The claims that were approved were all valid claims. The payments that went out the door were all valid claims. It was the banking information that was payments went to that was fraudulent. There was no fraudulent claims.

LEGISLATOR FORD: So you sent $710,000 to an incorrect bank account, okay, fraud, correct? So, how do you know right now when you make these payments to these bank accounts, okay, that it is an actual payment that this vendor was supposed to be paid?

MR. SCHOEN: We have the new controls in place and we reviewed all --

LEGISLATOR FORD: But you said there's limitations. You have no way of telling them what invoice it's for, right? You just deposit into their accounts. So people call up and they say hey, I got this $600,000 payment from you. Can you tell me what it's for?

MR. SCHOEN: Before the payment

PRECISE COURT REPORTING
(516) 747-9393 (718) 343-7227 (212) 581-2570
Finance 1-22-18

goes out the door we know exactly what the payment is for. We looked at all the backups in every invoice, all the backups before we make that payment and approve that payment. We know what the payment was for.

LEGISLATOR FORD: Like you did the $710,000?

MR. SCHOEN: Correct.

LEGISLATOR FORD: So you made a mistake there and you could make another mistake. I'm just saying now as you're moving forward.

MR. SCHOEN: That's why we have the additional controls in place.

LEGISLATOR FORD: What I'm saying though is, that I think that you really should firm that up so when you make these payments into people's accounts that there is a reason and that you know clearly and they know exactly what invoice to attribute that payment to. So they don't call you up and say hey, you sent me some money. What are you paying me for? Because you can then very well send it to some account and the people may say --
Finance 1-22-18

it might be a small mom and pop. Maybe the person is ready to leave Nassau County and now they're going to move to somewhere else, and all of a sudden they got a windfall of like $100,000 and you don't know that you paid them incorrectly and they're all of a sudden out the door. They got their plane tickets and they're gone. And you won't have the luck that you had with this bank, where ever it was, that told you that this account was an invalid account. And that thankfully we were able to recoup the money and I thank the Nassau County Police Department for their due diligence.

I see Comptroller that there are people who took credit for saving us from this debacle in regard to the $710,000. My ultimate question then would be in something like this, because it was a big breach and it's very unsettling for all of us, who's taking the blame?

MR. SCHNIRMAN: I would say very simply I don't think there's any credit to go around here. This was an attack, right? A
phishing attack on the county. This is something that we were targeted as a county. Others are being targeted the same.

From my perspective it's not a question of credit or blame. It's a question of continually improving our controls with the humility, as I mentioned earlier, of understanding that as we continue to improve them the scammers will continue to be more sophisticated. So this is an ongoing challenge for not just Nassau County but for municipalities all over the country.

LEGISLATOR FORD: You said though that you're also doing -- you had recent instructions or training for -- was this once again just with your cyber committee or was this actually with the employees to go over safeguards and what they can do? Because obviously we don't have this new system in place so that everybody has to be on their due diligence. Have you gone through with all of your employers training to let them understand what they need to do know to make sure that this does not happen again?
MR. SCHNIRMAN: As we said earlier, we have training within the comptroller's office and then there's been a broader training through the entire county by IT.

LEGISLATOR FORD: What has your office done to train your people?

MR. SCHNIRMAN: As we said, we did a training within the comptroller's office. You can speak to the details there.

MR. MARQUES: Yes, me, as fiscal officer, it is my responsibility over the Claims Division. We do on a periodic basis, I'd say every few weeks, discuss items like this in the news. For example, back in March where Google and Facebook were victims of this similar scam and lost about $125 million. Also Diesel Jeans another example case study. Mattel. All these companies have also been victims and we talk about that as a group.

We also look at opportunities to improve the system. We talk to each individual involved in the process and see
what they need, what tools they need, what
training they need to be better at what they
do. As the comptroller said, it's always
evolving and we always have to continue
training. It doesn't matter how much training
we need in the past we're going to continue to
do as much training as we need in the future.

LEGISLATOR FORD: I think it
better be done today because I think that this
is -- it was good news to recover this money.
I think it's bad news all around that even
happened. Thank you.

LEGISLATOR RHOADS: We will try
to make it quick for your benefit,
Legislator Ferretti.

Comptroller Schnirman, I have a
couple of concerns about the lack of
notification, particularly to the legislature,
that this incident even occurred. I happened
to find out through your press conference
almost three months after this incident
apparently took place in October and your
press conference I believe was on January
10th. Obviously, as the institution that
Finance 1-22-18

actually funds these accounts and as an institution that's charged with the oversight of county government, including the comptroller's office, I must admit I'm concerned.

You indicated that at some point in time you notified the county executive or at least the county executive's office. At some point in time you notified someone within the treasurer's office. At no point in time did you notify anyone at the legislature.

So can you please just walk me through the time frame, the time line of who knew what, when with regard to this incident and why it was that you chose to keep the information quiet for whatever time you did.

MR. SCHNIRMAN: So, as I mentioned earlier, we held a press conference with Commissioner Ryder. We were asked to not disclose information until that time as it has and still is an active investigation. As I had mentioned earlier, there were three to four other municipalities that were also targeted. We needed to recover the money
before the scammers could be alerted to that
and move the money themselves. So, from that
perspective, we had to wait to disclose to the
public until that time. I will mention --

LEGISLATOR RHOADS: I apologize

for interrupting. I'm not suggesting that you
needed to notify the public. What I'm
suggesting is that you need to notify your
other partners in government that there's a
situation.

MR. SCHNIRMAN: We were

immediately in touch with the police
department.

LEGISLATOR RHOADS: Did the

police department tell you not to notify the
legislature?

MR. SCHNIRMAN: The police
department asked us to not do notification and
I will just leave it there.

LEGISLATOR RHOADS: To whom? To

anyone?

MR. SCHNIRMAN: We were asked not
to speak about the incident.

LEGISLATOR RHOADS: If I were to
Finance 1-22-18

ask the police department, a representative
from the police department, whether the
instructions to the comptroller's office
included not notifying the county
legislature?

MR. SCHNIRMAN: I will leave it there for now.

LEGISLATOR RHOADS: Who within the police department gave you the notification?

MR. SCHNIRMAN: Excuse me. Can you repeat the question.

LEGISLATOR RHOADS: You indicated that someone within the Nassau County Police Department gave you the instruction not to notify the county legislature. Who was it?

MR. SCHNIRMAN: Our conversations with the police department were obviously between myself and the commissioner and deputy comptroller spoke to the team as well.

LEGISLATOR RHOADS: So it's your --

MR. SCHOEN: There were concerns to protect the integrity and the investigation
as to not disclose the information to as little amount of individuals as possible because the money moves fast and because there was a need to recover the money before it went anywhere else. That's what was conveyed to us.

LEGISLATOR RHOADS: Was a specific instruction given to you by the Nassau County Police Department not to notify the county legislature of this incident?

MR. SCHNIRMAN: I don't know that the legislature was discussed as part of that operational -- in terms of operations.

LEGISLATOR RHOADS: Who did the police department tell you was important enough for you to be able to inform?

MR. SCHOEN: I think you can talk to them about their investigative techniques but I believe it's --

LEGISLATOR RHOADS: I'm not asking about techniques. You're telling me that you received specific instructions from the Nassau County Police Department not to disclose information. I understand not to
disclose information publicly. I'm asking you what specific instructions did you receive not to disclose information to your other partners in government? Not publicly. If you want to talk to us now in executive session. Same conversation could have been had in executive session. Same conversation could have been had in private.

I want to know did you receive a specific instruction whether and when you were permitted to notify the county executive, whether and when you were permitted to notify the county treasurer and whether and when you were permitted to notify the county legislature and who gave you that instruction?

MR. SCHOEN: There were no specific instructions. There was a general instruction to limit the amount of individuals who are aware of the information so that we can catch the perpetrator.

LEGISLATOR RHOADS: So it was not the Nassau County Police Department that gave you that instruction, it was the comptroller's
Finance 1-22-18

office that made the decision that you
couldn't notified the county legislature?

MR. SCHOEN: As the comptroller
said, the county legislature did not
specifically enter into that conversation.

LEGISLATOR RHOADS: When was the
county executive's office notified?

MR. SCHOEN: As soon as we were
informed of the fraudulent account and
identified the additional payments.

LEGISLATOR RHOADS: That would
have been once you got a telephone call from
the bank?

MR. SCHOEN: Once we were
notified from the bank.

LEGISLATOR RHOADS: That
notification came through a telephone call,
didn't it?

MR. SCHOEN: It came from an
electronic communication.

LEGISLATOR RHOADS: Email?

MR. SCHOEN: Yes.

LEGISLATOR RHOADS: You received
the email. County executive's office got
Finance 1-22-18

notified right away. Who within the county executive's office did you notify?

MR. SCHNIRMAN: I think we are not going to speak to the details of who talk to who when and how and what.

LEGISLATOR RHOADS: Why?

MR. SCHNIRMAN: Outside of executive session we're not going to get into the details of how the incident was handled in that sense.

LEGISLATOR RHOADS: How can disclosure of that information jeopardize any investigation?

LEGISLATOR SOLAGES: At this moment I would like to make a motion for this to be in executive session. Clearly a skilled defense attorney for these perpetrators can use this information and that would affect an investigation. At this moment I would like to make a motion to go into executive session.

LEGISLATOR KOPEL: I don't think we're worried about protecting the defendant or the perpetrator over here. I don't think that's what the questions were directed to.
Finance 1-22-18

Mr. Rhoads.

LEGISLATOR SOLAGES: Clearly this relates to senior staff performance and it also relates to attorney consultation. For those reasons, I'm making a request for executive session.

LEGISLATOR KOPEL: Okay. We have a motion. We have a second?

LEGISLATOR RHOADS: I can move on with other questions.

LEGISLATOR KOPEL: Why don't we do that and you'll make your motion again. Or somebody will make a motion again and then we will do it.

LEGISLATOR RHOADS: Who was notified and when is in executive session.

I just want to clarify what, and a couple of my colleagues here have gone into it, the Newsday article from your press conference indicates, quote, Nassau County Comptroller Jack Schnirman said controls in place at the comptroller's office immediately identified the fraudulent activity leading the funds to be frozen. He said the additional
Finance 1-22-18

security controls had been added -- that
additional security controls had been added
since the attack.

That isn't accurate as we now know, correct?

MR. SCHOEN: Once we were notified by the bank that there were monies going into the fraudulent account we were able to immediately identify the $710,000 and we immediately took action and started the investigation.

LEGISLATOR RHOADS: But the suggestion that there was some sort of internal control in place at the comptroller's office that actually discovered this would be inaccurate.

MR. SCHOEN: We were able to identify the $710,000 as effectively and as fast as we were based on the records we maintained in our office. Part of our controls are to have those records so we can get the money back as quickly as possible.

LEGISLATOR RHOADS: Were it not for the fact that somebody at the bank, not an
employee of Nassau County, not an employee of the comptroller's office, were it not for somebody on the ball at the bank who picked up on this you would have had absolutely no idea that this even happened perhaps until the vendor called up and said where's my check. Is that accurate?

MR. SCHOEN: It's perspective, yes.

MR. SCHNIRMAN: I will just answer. As the deputy comptroller had said earlier, that is part of our controls.

LEGISLATOR RHOADS: Part of your controls is relying on some third party happen to catch it? That's what your control is?

MR. SCHNIRMAN: That's your characterization of it. However --

LEGISLATOR RHOADS: But that's what happened, right?

MR. SCHNIRMAN: A major piece obviously of anyone's controls is working with the financial institutions.

LEGISLATOR RHOADS: Just out of curiosity, since that's apparently one of our
controls, according to Open Checkbook -- and this is by the way isn't something that happened just once, right? I think we've established in the testimony today that there were multiple submissions adding up to the $710,000; is that correct?

MR. SCHOEN: No. Again, it's one vendor's profile that got phished and modified.

LEGISLATOR RHOADS: But there were multiple --

MR. SCHOEN: -- payments that went to that vendor profile, yes.

LEGISLATOR RHOADS: Multiple payments that --

MR. SCHOEN: All legitimate claims. No fraudulent claims. All the claims were legitimate claims reviewed and approved by the comptroller's office.

LEGISLATOR RHOADS: How many payments went to the wrong destination?

MR. SCHOEN: There were multiple payments comprising the $710,000.

LEGISLATOR RHOADS: How many
Finance 1-22-18

payments went through before the bank caught this?

MR. SCHOEN: That's the level of detail we would like to give you in executive session.

LEGISLATOR RHOADS: I'm just curious at how many things got past us before somebody outside the county picked this up?

MR. SCHOEN: There were multiple payments. Not many but multiple. All within a less than 30 day period.

LEGISLATOR RHOADS: Was it more or less than five?

MR. SCHOEN: Less than ten.

LEGISLATOR RHOADS: The updated controls that you put in place, you're telling us you can't discuss those updated controls unless we're in executive session?

MR. SCHOEN: We discussed a number of them.

MR. SCHNIRMAN: We went into quite a bit of detail on them already.

LEGISLATOR RHOADS: On certain of them. Is that an exhaustive list of the

PRECISE COURT REPORTING
(516) 747-9393 (718) 343-7227 (212) 581-2570
updated controls that you put in place?

MR. SCHOEN: I don't recall all
of them that were mentioned during the
proceeding today but it's pretty exhaustive I
would say or nearly there.

LEGISLATOR RHOADS: We've
discussed Open Checkbook and the information
that is part of some of these controls you're
now requiring. In this particular instance
you indicated that the scammer completed the
form with the correct tax identification
number, the correct vendor name, the correct
vendor contact name, the correct vendor
address and the correct vendor phone number,
right?

MR. SCHOEN: And submitted the
modified fraudulent check.

LEGISLATOR RHOADS: And a copy of
the check. The information that's contained
here as you're check against that is
information that can be publicly obtained
probably within about 20 minutes. What other
controls are you putting in place or checks
are you putting in place to safeguard against
MR. SCHOEN: As discussed, we do the dual check. With this one individual or an individual at the vendor who will request the change. And then our department will reach out to a separate individual within the vendor, at the vendor, preferably the contact person on the contract, to verify those changes are being made and verify all of the information on the form.

LEGISLATOR RHoads: If it was simple enough for this particular fraudster, I guess we're calling him, to be able to game the system, how do you have any confidence that the 120,738 checks that were issued to vendors that the same thing didn't happen multiple times that the bank didn't happen to tell us about?

MR. SCHOEN: Or the vendor not telling us they didn't receive payment, right?

LEGISLATOR RHoads: What safeguards do we have that that hasn't occurred?
Finance 1-22-18

MR. SCHNIRMAN: I think we have been over this.

MR. SCHOEN: We have the additional controls we put in place. We reviewed all of the forms that were submitted for a six month period prior to the incident and verified all that information was accurate for all the active vendors.

LEGISLATOR RHOADS: I guess we'll get the rest of the answers in executive session.

LEGISLATOR KOPEL: Mr. Ferretti.

LEGISLATOR FERRETTI: Thank you Chairman. Good afternoon gentlemen. I want to get some dates down. Number one, what date were you first notified of this incident?

MR. SCHOEN: As indicated, we will give specifics like that in executive session.

LEGISLATOR FERRETTI: I was just asking what date they were notified of the incident.

LEGISLATOR KOPEL: Why don't you do this? Have you been making notes of these
questions, of these important questions that you didn't want to answer? Yes?

MR. SCHOEN: Not didn't want to answer but thought it was necessary to answer in executive session, yes.

LEGISLATOR KOPEL: Understood.

I'm sorry. Forgive me. Correct. You are absolutely correct. You're making notes. Do we have your undertaking to supply those answers in a confidential note to the committee?

MR. SCHNIRMAN: Sure.

LEGISLATOR KOPEL: When?

MR. SCHNIRMAN: As soon as we can put them together.

LEGISLATOR KOPEL: A day, a week, a year?

MR. SCHNIRMAN: Within a week.

LEGISLATOR KOPEL: Fair enough.

LEGISLATOR FERRETTI: Can you tell us if you first discovered this before or after the budget was passed by this body? The county budget.

MR. SCHOEN: A particular year?
Financial 1-22-18

LEGISLATOR FERRETTI: The 2020 budget that we passed in October 2019.

MR. SCHOEN: I don't recall the date that the budget was passed.


MR. SCHOEN: The answer will be in the memo that we provide to you.

LEGISLATOR FERRETTI: Do you recall informing Newsday, anyone from your office, that you called the police about this issue on October 25, 2019? In a press release?

MR. SCHNIRMAN: I believe the police commissioner may have informed them of that but that date sounds right.

LEGISLATOR FERRETTI: Right in terms of what? When you called the police? When somebody from your office called the police?

MR. SCHNIRMAN: Correct.

LEGISLATOR FERRETTI: We know you contacted the county executive at some point after discovering this, correct? County
Finance 1-22-18

executive's office?

MR. SCHNIRMAN: Correct.

LEGISLATOR FERRETTI: Was that before or after you contacted the police?

MR. SCHNIRMAN: I think basically simultaneously but.

LEGISLATOR FERRETTI: What does that mean "simultaneously"? You had two phones going?

MR. SCHNIRMAN: No. That's the level of detail we're going to speak to you today.

LEGISLATOR FERRETTI: Will you include that information in your memo to us?

MR. SCHNIRMAN: Sure.

LEGISLATOR FERRETTI: Can you explain what a cyber attack is?

MR. SCHNIRMAN: I think we spoke to it earlier as we began. That there are multiple kinds of cyber attacks and we were clear about in this instance that this was a phishing attack rather than an overall attack on the county's IT infrastructure.

LEGISLATOR FERRETTI: So then you
Finance 1-22-18

would say a phishing attack is a type of cyber attack, would that be fair?

MR. SCHNIRMAN: We've mentioned that several times, yes.

LEGISLATOR FERRETTI: I understand. I might ask some questions that you've already answered. I apologize for that. It's been a couple of hours.

My understanding of what a phishing expedition is is a fraudulent email or communication that draws information from the municipality in this case. Would you agree with that?

MR. SCHOEN: That's fundamentally what happened here. There was a fraudulent email, the mimicked email that drew the information from the municipality.

LEGISLATOR FERRETTI: What information did it draw? You didn't give them a credit card number. You didn't give a social security number. What information did it draw?

MR. MARQUES: Essentially they requested and received a vendor information
Finance 1-22-18

form which is publicly available on our website.

LEGISLATOR FERRETTI: Okay. So then in what way is this a phishing expedition?

MR. SCHOEN: The form was completed and submitted using the phisher's mimicked email account.

LEGISLATOR FERRETTI: Right. But they got information from you that's public information, correct?

MR. SCHOEN: Somewhat semantics.

LEGISLATOR FERRETTI: I don't think it is. You had a press conference on January 11th indicating that somehow you uncovered a phishing expedition and cyber attack. And I'm trying to determine if there really was even a phishing expedition at all or whether you just sent money to the wrong bank account.

MR. SCHOEN: The information was submitted using the mimicked email account. The initial information from that mimicked email account was sufficient. They asked the
Finance 1-22-18

to send the information, the form, which was then completed and sent back to us using that mimicked email account.

LEGISLATOR FERRETTI: What's asked? You indicated they asked the fiscal officer. Was the initial email to the fiscal officer?

MR. SCHÖEN: The initial email was to a general email account at the comptroller's office which was forwarded to the fiscal officer.

LEGISLATOR FERRETTI: Was that email addressed to the fiscal officer?

MR. SCHÖEN: It was to a general email account.

LEGISLATOR FERRETTI: I know you're saying it was sent to a general email but did it indicate --

MR. SCHÖEN: That's a level of detail that we will provide in our report.

LEGISLATOR FERRETTI: I can tell you I have copy of it. So, what I can tell is if my seven year old son got an email like this he wouldn't have responded to it. It's
Finance 1-22-18

very hard to believe that your office did.

But can you tell me again -- I'm sorry. When
you received the email are there any dual
controls in place?

MR. SCHNIRMAN: I'm sorry.

Excuse me Legislator. You just said you had a
copy of which now?

LEGISLATOR KOPEL: Mr. Ferretti, you have a copy of that email?

LEGISLATOR FERRETTI: Yes.

LEGISLATOR KOPEL: Can you
circulate it?

LEGISLATOR FERRETTI: Sure.

MR. SCHNIRMAN: Can I ask how and
why you have a copy of that email?

LEGISLATOR FERRETTI: It was
given to me a few minutes ago.

MR. SCHNIRMAN: By whom?

LEGISLATOR FERRETTI: I get to
ask the questions Comptroller respectfully. I
will send you a memo when I get the
information.

MR. SCHNIRMAN: I get to be
cconcerned about the security here and that's a
Finance 1-22-18

LEGISLATOR FERRETTI: Security of an email that was sent to your general email address?

MR. SCHNIRMAN: We're talking about internal emails that are the subject of an investigation. So that is a concerned if they're being forwarded around, yes.

LEGISLATOR FERRETTI: I think that we should be concerned about what happened a little bit more than how I'm trying to get to the bottom of why it happened.

MR. SCHNIRMAN: Well, I think we can agree that we should be concerned about what happened and I think we are concerned about what happened and there's a point where the concern about what happened --

LEGISLATOR KOPEL: I think we're running in circles here and this is another illustration of the fact that if you think this shouldn't be out there well, then the fact that it is out there is not a great thing.

LEGISLATOR FERRETTI: I think we
Finance 1-22-18

should move.

LEGISLATOR KOPEL: And maybe not a great thing from your office. I don't know.

LEGISLATOR FERRETTI: Were there dual controls in place when emails such as these came in?

MR. SCHOEN: I'm not sure we understand the question.

LEGISLATOR FERRETTI: When this, as you described it, phishing email came in, prior to the change being made to the bank account information were there more than one set of eyes that reviewed this request?

MR. SCHOEN: Yes.

LEGISLATOR FERRETTI: Who from your office, what title if you're not going to give me a name, reviewed the request?

MR. MARQUES: The initial email was sent to that general mail box. It was then forwarded to me by the director of accounting. I then had possession of it. And once the information was provided, submitted that to a supervisor over that unit who then forwarded it on to a person to process it.
LEGISLATOR FERRETTI: I apologize if this was already asked. It may have been. But was there any kind of contact, whether by telephone or any other means, with the vendor prior to making the change to confirm that they were requesting this change?

MR. SCHOEN: At the time the major control in place was the submittal of a void check which was fraudulently submitted. The additional controls were put in place to make that contact.

LEGISLATOR FERRETTI: Is that a no? There was no communication with the vendor to confirm that they were requesting this change?

MR. SCHOEN: Correct.

LEGISLATOR FERRETTI: When you say there was a void check that was sent to the comptroller's office, was that void check from the old account or the account that they were looking to change to?

MR. SCHOEN: Change to.

LEGISLATOR FERRETTI: So how does that safeguard anything?
Finance 1-22-18

MR. SCHOEN: We put in additional controls in place that we discussed.

LEGISLATOR FERRETTI: So it doesn't? Getting a check from the new account does nothing, correct?

MR. SCHOEN: It enabled us to verify that it is in fact a true bank account.

LEGISLATOR FERRETTI: That's great. But how does that in any way -- you included it on your packet, on your slide show. How does that in any way safeguard this from happening, getting a copy of the check? You didn't contact the vendor to confirm they wanted this change. You got a check that we now know was for the new account which is useless. In what way did this check -- I guess I just said it was useless. Would you agree? Did this check act as a safeguard in any way whatsoever?

MR. MARQUES: It didn't. I will explain that. When that control was initiated, the comptroller's office was made aware in three separate instances, three separate vendors. What it does is it ensures
that the vendor doesn't make any mistakes in
providing their own bank account information
and verifies that the numbers provided to us
are correct and accurate.

LEGISLATOR FERRETTI: You lost
me. Are you saying you verified the new
account number that they wanted with the check
to confirm that there was no error like typo
in the numbers, is that what you're saying?

MR. SCHOEN: Correct.

LEGISLATOR FERRETTI: To be
clear, you verified the new account they
requested with a check to make sure that they
didn't improperly enter the new account
number?

MR. SCHOEN: And the information
on check matched the vendor information.

LEGISLATOR FERRETTI: Okay. But
that doesn't stop or provide a level of
security to prevent what happened here,
correct? That just prevents an incorrect
account number on the new account.

MR. SCHOEN: Prevent a
sophisticated individual from mimicking a bank
check with the correct address and a correct account number, no.

LEGISLATOR FERRETTI: You indicated that you've already met with the IT department; is that correct?

MR. SCHOEN: No.

LEGISLATOR FERRETTI: I thought you said in the beginning that you've already met with them in terms of new training procedures.

MR. SCHOEN: They've instituted new training procedures as well as we have.

LEGISLATOR FERRETTI: Has your office contacted IT since October 25, 2019 with regard to training comptroller's employees?

MR. SCHOEN: We've been doing internal training and on top of that the IT department has been training for all county employees on how to identify phishing. And we are working with the IT department to have the 700 form or the vendor information form submitted through the vendor portal.

LEGISLATOR FERRETTI: Just to be
clear, the new procedures and policies that you put in place after this attack you're not willing to share them right now to the public; is that correct?

MR. SCHOEN: No. I think we have.

LEGISLATOR FERRETTI: All of them?

MR. SCHOEN: I believe so.

MR. SCHNIRMAN: I think we shared the general thrust of them in some significant level of detail to the extent that we could and we also detailed additional levels of control that are forthcoming.

LEGISLATOR FERRETTI: How can you ensure that this hasn't happened before? Strike it. Let me ask you again. Are you aware of this ever happening in Nassau County? Has the Nassau County Comptroller's Office ever been the subject of a scam such as this?

MR. SCHNIRMAN: During my time? I'm not aware.

LEGISLATOR FERRETTI: I'm not
Finance 1-22-18

asking during your time. Are you aware of any
time the Nassau County Comptroller's Office
ever being subject to a scam such as this?

MR. SCHNIRMAN: Broadly speaking

no.

LEGISLATOR FERRETTI: How about

any of the other 62 counties in New York

State?

MR. SCHNIRMAN: I'm not in a

position to answer comprehensively for New

York State. But as we spoke about earlier in

the presentation, we are seeing attacks

proliferate. In fact, in this particular

attack alone there were three to four

municipalities targeted. Some of which on

Long Island.

LEGISLATOR FERRETTI: Sorry. I'm

getting a little distracted. I'm not asking

you to answer for all of New York State. What

I'm asking you is, are you aware of any other

counties who have been attacked in a similar

way? If the answer is you're not aware of it

that's fine. I'm just asking if any of the

three of you are aware.
MR. SCHOEN: We're aware that in this instance there were other counties attacked in a similar manner.

LEGISLATOR FERRETTI: What counties?

MR. SCHOEN: That's not a level of detail we will provide in public.

MR. SCHNIRMAN: I believe the police commissioner -- hang on a moment. I believe it was disclosed that there was a municipality within Suffolk County that was attacked.

LEGISLATOR FERRETTI: So it wasn't the county then? It's a local municipality within Suffolk County?

MR. SCHNIRMAN: I believe that is the case. In addition, this morning I'm aware that the county itself disclosed that it was attacked. Not in this particular incident. In a separate incident.

LEGISLATOR FERRETTI: Did your office ever contact NIFA with regard to this attack prior to the press conference that you had on January 11th?
Finance 1-22-18

MR. SCHNIRMAN: I don't believe so but I will double-check.

LEGISLATOR FERRETTI: So there's a chance you contacted NIFA with regard to this attack? You can't tell me affirmatively that you did not?

MR. SCHNIRMAN: I don't believe that we did but I will double-check.

LEGISLATOR FERRETTI: Did your office contact anyone outside of Nassau County government about this attack prior to January 11th?

MR. SCHOEN: Other than the bank that would have been involved there would have been no one --

LEGISLATOR FERRETTI: They contacted you, right?

MR. SCHOEN: -- that I can recall. But when you say contact, you're talking about general contacts?

LEGISLATOR FERRETTI: You didn't tell us. Did you tell anyone else?

MR. SCHOEN: Contacts regarding the incident. So we would have had to talk to
Finance 1-22-18

the bank about the incident. That's a contact.

LEGISLATOR FERRETTI: Other than the bank. Anyone outside of Nassau County government did you contact them about this incident prior to January 11th?

MR. SCHNIRMAN: I don't believe so.

LEGISLATOR FERRETTI: Again, you can't say affirmatively you did not?

MR. SCHOEN: We may have asked some information from the vendor but I don't recall.

LEGISLATOR FERRETTI: I just want to be clear here because I think this is important. You cannot say whether or not on 100 percent certainty, I'm asking you Comptroller, whether somebody from your office or you personally contacted NIFA and informed them of this? The fiscal control board of this county, you being the fiscal watchdog, you can't tell me if you contacted NIFA and informed them prior to them approving our budget that this incident occurred?
Finance 1-22-18

MR. SCHNIRMAN: No, I cannot say that definitively we contacted NIFA. And if you would like to delineate what you see as a tie-in between this and the budget I'd be interested in where you're coming from.

LEGISLATOR FERRETTI: Sure. When we past the budget and possibly when NIFA approved budget, we don't know because you don't know if you told them, we were not aware of this possible deficiency shortfall in our budget. You don't see that as a problem?

MR. SCHNIRMAN: I think you're making a link between payments and budget that is incorrect.

LEGISLATOR FERRETTI: So if this money was not recovered does the vendor get paid?

MR. SCHOEN: Fortunately that's not a road we had to go down.

LEGISLATOR FERRETTI: We can thank the bank for that. But the question is, if the money wasn't recovered would the vendor have gotten paid?

MR. SCHOEN: The vendor would
have had a valid claim against the county and money would have been due and owing.

LEGISLATOR FERRETTI: Right. And who pays that? It's taxpayer money, correct?

MR. SCHNIRMAN: Correct.

LEGISLATOR FERRETTI: So, we voted on a budget where there was this money in limbo where you did not know if we were going to recover it and we were not informed of that prior to voting. We also didn't know the amount at that time if I'm following this correctly. We didn't know it was limited to $710,000.

MR. SCHNIRMAN: I'm sorry. I'm not following that this is relevant to the budget of 2020. First of all, this was a 2019 financial issue. I think you're conflating the two things and I don't think they actually go together.

LEGISLATOR FERRETTI: Then maybe I'm mistaken. But if there's a shortfall in the 2019 budget wouldn't it come out of the 2020 budget?

MR. SCHNIRMAN: If there was a
shortfall in the 2019 budget it would be dealt with from a fund balance perspective which is an entirely different discussion altogether. But it would not necessarily impact the 2020 budget.

LEGISLATOR FERRETTI: Doesn't the fund balance go into the budget?

MR. SCHNIRMAN: The overall fund balance of the county -- I don't believe that it would impact the budget. Bottom line I don't see that these two issues --

LEGISLATOR FERRETTI: That is a discussion we could have had.

MR. SCHNIRMAN: I don't see that these two issues are related.

LEGISLATOR FERRETTI: When the budget was passed do you know what the exposure was? On October 28th did you know what the exposure was to the 2019 or 2020 budget?

MR. SCHNIRMAN: I believe at that point the funds were frozen.

MR. SCHOEN: The majority of the money at that point would have been recovered.
LEGISLATOR FERRETTI: But can you confirm that that was -- we're talking about a three-day period here, right? You notified the police on October 25th. We passed the budget on October 28th. Are you telling me in those three days, which, by the way, I think two of them were a weekend, but I'm not sure about that, that you were able to confirm with 100 percent certainty that the exposure was limited to $710,000?

MR. SCHOEN: Yes.

LEGISLATOR FERRETTI: From just this incident or did you do an audit where you went back and determined if anything else happened to other vendors?

MR. SCHOEN: We confirmed six months worth of vendor information forms to make sure they were correct.

LEGISLATOR FERRETTI: That's all I have for now. Thank you.

LEGISLATOR SOLAGES: To the Chair, point of order. Legislator Ferretti asked -- presented this email that I learned off the record that it was obtained from the
police department. I'd just like to know when and where did you receive that documentation?

LEGISLATOR KOPEL: I'm sorry, you're asking him?

LEGISLATOR SOLAGES: Legislator Ferretti mentioned that he received a copy of the actual email that was used in this alleged scheme.

LEGISLATOR KOPEL: You saw it as well.

LEGISLATOR SOLAGES: I would like to know how that document --

LEGISLATOR KOPEL: I will answer you. Counsel --

LEGISLATOR SOLAGES: Our counsel didn't receive a copy of it.

LEGISLATOR KOPEL: You want to let me finish my sentence or would you rather just keep on making speeches?

LEGISLATOR SOLAGES: I'm asking questions.

LEGISLATOR KOPEL: Now, counsel requested that the police department show it to him. Police department agreed to show it
to him on a confidential basis.

LEGISLATOR SOLAGES: He put it on the record.

LEGISLATOR KOPEL: It was not provided in a confidential basis. It was provided to us and we just showed it to you too. There's nothing nefarious. We just saw it for the first time and we showed it to you for the first time. None of the members of the committee saw it before now. We just saw it for the first time and so did you. There is nothing scary about this.

LEGISLATOR SOLAGES: Was it the first time that Mr. Ferretti saw it?

LEGISLATOR KOPEL: Mr. Ferretti, was it the first time you saw it?

LEGISLATOR FERRETTI: Absolutely.

LEGISLATOR KOPEL: Everybody sitting here saw it for the first time. I just saw it for the first time.

LEGISLATOR SOLAGES: Can we receive an official copy? Can our counsel receive an official copy?
LEGISLATOR KOPEL: Yeah. If the PD allows it fine with us. The police will be out here and we will ask them for it. Because we asked for it and you didn't. It's not that complicated.

LEGISLATOR SOLAGES: This is a public hearing. Why wouldn't both sides have it?

LEGISLATOR KOPEL: Because we asked for it and we got it and you didn't. And when we got it we looked at it and showed it to you too. It's really not complicated here. You want to make something out of nothing you can keep on trying.

By the way, I just would make one point as to what that did show. There was a real red flag on that email and I'm not going to go into depth on it but this is a very simple thing. The signature -- the from of the scammer showed that it came from X Corp. dot org and right down at the bottom it showed the www of that same company, that same corp. dot com, which showed that they had a dot com, and that conflict that's a real red flag. But
Finance 1-22-18

it was missed. In any event, Ms. Walker.

LEGISLATOR WALKER: I just have one quick question. Not who you told when or whatever. But don't you think before you had a press conference with Newsday it would have been nice for the legislators, shouldn't even use the word nice, should be something that this body should know about before we read it in Newsday? I mean, I just think that would be proper protocol. You are the Nassau County Comptroller and you don't feel that's important to share with the legislature? We see it in a newspaper.

MR. SCHNIRMAN: We shared it all at once and I appreciate your request and that's something that will certainly be taken into consideration going forward.

LEGISLATOR WALKER: Could I ask you, did you know before you saw it in Newsday? Did any of you know before you saw it in Newsday?

LEGISLATOR BIRNBAUM: I would just say there are lots of things in this county that we don't hear about before we see
Finance 1-22-18

in Newsday that I've found in the past. It's not just this one time. It's several items that we don't get informed about.

LEGISLATOR WALKER: Right. I agree. There are many things we see and it doesn't make me happy. I just think this is extremely important. And for us to find out by seeing it in Newsday I have a big problem with that. I've stated before I've had a problem with it. So I'm stating it publicly here that I have a major problem with that.

So you knew nothing either before you saw it in Newsday.

LEGISLATOR KOPEL: Gentlemen, thank you so much for coming. We have some Advil available if you'd like on the way out. But otherwise you are free. I would ask you not to leave the room actually because I'm told that there may be some further questions that may develop. So if you would just hang out that would be preferable.

We have one more witness I believe from IT. That would be Nancy Stanton. Just state your name and position for the record.
Finance 1-22-18

MS. STANTON: Nancy Stanton.

LEGISLATOR KOPEL: You got that already? Go ahead.

MR. PEREZ: Al Perez, deputy commissioner.

MR. BARROW: Steve Barrie, manager, computer operations.

LEGISLATOR KOPEL: Do you have a statement to make?

MS. STANTON: I do.

LEGISLATOR KOPEL: Please go ahead go.

MS. STANTON: Good evening.

Nancy Stanton, IT commissioner. We would like to thank you for this opportunity to speak here today to discuss efforts that my department have put in place to harden our infrastructure. I have brought with me today senior staff Al Perez and Steve Barrie.

Let me first begin by letting you know that the Department of Information Technology takes cyber security very seriously. The infrastructure, network systems and house data we store and maintain
in county are the cornerstones for the
operation of many departments and
constituents. Because of this, it is one of
the most if not the highest priority in my
department. My department is committed to
reduce security risks by eliminating potential
attacks throughout the county.

During 2018 and 2019, through a
grant, we were fortunate and pleased to work
with the Department of Homeland Security for a
cyber security evaluation. The purpose of
this cooperative exercise was to assess any
possible vulnerabilities that we have had in
our system. This analysis produced a report
of vulnerabilities and recommendations to
harden our environments and systems. As of
today, I'm pleased to say that with the
support of my staff all critical
recommendations have been remediated.

In addition to meeting weekly to
discuss security measures and weekly activity,
we have done many things. Some you can see.
Some you cannot. Here are a few examples of
what you can see.
1 Finance 1-22-18
2 Actively migrating from Windows 7
to Windows 10. Acquired and deployed user
employee security training. Implemented
multifactor authentication across a number of
departments soon to be countywide.
3 Implemented a complex password policy. Lock
down the use of personal email access.
4 Limited web access through web filters.

Here are a few things you cannot
see. Implemented stronger application of date
deployments, browser Windows versions.
5 Adopted a more aggressive security update
practice with Windows and MS office security
updates. Acquired and deployed countywide AI
driven security suite and maintain version
6 deployments.

Overhauled completely the way
Nassau County performs backups. Full server
7 machine backups using the latest version and
all available backup agents automatically are
8 in place.

Server OS security patching is
9 currently being implemented. Our firewalls
10 now have deep SSL scanning enabled for network
Finance 1-22-18

vulnerabilities.

In June of 2019 there was a local law 229-19 to enacted through this legislative body to provide the following which I will now give an update.

Employee training. This is underway. We expect to be complete by the end of January. Going forward we will be doing this training on a semiannual basis. Also to note, we have conducted many cyber security seminars to constituents throughout the county. We will also begin a program where these seminars are offered to employees.

Number two. Submit an annual cyber security risk assessment and response analysis. This is in progress. We have engaged a vendor to assist with penetration testing and reporting. Once a report is complete it will be forwarded accordingly.

Three. Establish a panel of security service and incident response providers to assist --

LEGISLATOR KOPEL: Ms. Stanton.

Forgive me. We all appreciate all these
Finance 1-22-18

things but do you think you might be able to
confine your remarks to the implementation of
various controls that would apply to the
comptroller rather than as a countywide? In
other words, it's very important what you're
doing and I don't mean to denigrate that at
all. But this hearing is pretty narrowly
focused. So, if you have any light that you
can shed on the recent event that we've been
discussing. I assume you've been here. A.

And B, as to what you may have
implemented or would like to suggest to
implement in order to prevent a recurrence
that would be great. Thank you.

MS. STANTON: We are working with
the comptroller's office as far as registering
vendors, providing passwords so that they can
only get in. We are working with them on the
700 form, which they mentioned, to be online
and in order to access that you would have to
have a password.

Employee training. We are already
doing. You guys mentioned encryption. We
would be happy to work with them on that.
LEGISLATOR KOPEL: You haven't had any requests for that?

MS. STANTON: We have several departments or agencies using very minimally. But we certainly should be --

LEGISLATOR KOPEL: But there's not been any request yet from the comptroller specifically for that?

MS. STANTON: There has not.

LEGISLATOR KOPEL: Is that something that you consider important?

MS. STANTON: Yes. For them yes.

LEGISLATOR KOPEL: Go on please.

MS. STANTON: That's it. We were not involved in the recent event.

LEGISLATOR KOPEL: You have no ideas of -- okay, good. Can you give us any good ideas as to what you think ought to be implemented based upon what you've heard here today beyond whatever we might have suggested?

MS. STANTON: We can talk with them with whatever they need and certainly help implement whatever they need.
LEGISLATOR KOPEL: A multifactor authentication going to them regardless.

MS. STANTON: They have that already. That's in place. It is being rolled out throughout the county. The training is being rolled out.

LEGISLATOR KOPEL: The encryption obviously. Is there a VPN in place for their transactions?

MR. BARRIE: No. There's no VPN in place for their transactions.

LEGISLATOR KOPEL: Would you not suggest that there ought to be?

MR. BARRIE: In what way would you think that?

LEGISLATOR KOPEL: I guess that just an additional layer of protection against somebody hacking in, observing emails that are going in and out.

MR. BARRIE: The VPN would be for if there were transactions coming in and out of the county, not for emails. It would be if somebody was connecting --

LEGISLATOR KOPEL: VPN would
Finance 1-22-18

not --

MR. BARRIE: Would not alleviate this issue no.

LEGALISATOR KOPEL: Emails would not travel through the VPN?

MR. BARRIE: No.

LEGALISATOR KOPEL: If you had a VPN?

MR. BARRIE: Our email system in Nassau County is in Microsoft Office 365. So anything in and out of the county is coming over our Internet connection.

LEGALISATOR KOPEL: Which is adequately protected in and of itself, therefore the VPN -- okay. It's protected from snooping. Got it.

MR. BARRIE: Like Mr. Schnirman said, it was a phishing attempt on the comptroller's office. So last week we actively blocked 1100 phishing attempts into the county.

LEGALISATOR KOPEL: Can you set things up at the comptroller's office, if necessary, so that nothing is done from a
remote computer?

MR. BARRIE: Nothing is done --
LEGISLATOR KOPEL: No financial transactions can be implemented through a remote computer.

MR. BARRIE: If financials transactions, if they're coming from outside the county they can only come through a VPN or a secure connection.

LEGISLATOR KOPEL: I'm talking about -- in other words let's say, I'm just imaging this, there's no suggestion that this has actually occurred just to be clear, but should a county employee decide to work from home let's say and process payments. By coming in through the county system --

MR. BARRIE: They will be coming in through a VPN.

LEGISLATOR KOPEL: They will be coming in through a VPN.

MR. BARRIE: Correct.

LEGISLATOR KOPEL: Therefore that would be safe?

MR. BARRIE: Correct.
LEGISLATOR KOPEL: Anybody?

Thank you. Now we're done with our witnesses and if there are any members of the public that would like to comment you're welcome to let yourselves be known now. Anybody? We have a winner here. You would like to make a public comment? Why don't you come right up please.

MS. HESSION: My name is Eileen Hession and I come from Long Beach. I'm really up here just to say thank you very much for having this hearing. I come from Long Beach where we are in deep financial trouble.

It was stated that this was an attempted scam but it was actually a successful scam, and I want to thank the bank who discovered it and reported it. Otherwise we'd be out $700,000.

In Long Beach we had few financial things in place that took care of our finances. We were fed much misinformation regarding the city's finances. No checks, no balances, inadequate safeguards and incompetence. Long Beach taxes have risen
substantially. No one has ever taken responsibility for it and no one has ever said the buck stops here.

I want to sincerely thank you, the legislature, for holding this hearing transparently and looking to strengthen all controls and procedures. Thank you to the bank and thank you again to the legislature.

LEGISLATOR KOPEL: Thank you.

Anyone else? I'm going to take a motion to adjourn by Ms. Birnbaum. Seconded by Ms. Walker. All those in favor of adjourning? Any opposed? We are adjourned.

Thank you everyone.

(Meeting was adjourned at 5:25 p.m.)
CERTIFICATION

I, FRANK GRAY, a Notary Public in and for the State of New York, do hereby certify:

THAT the foregoing is a true and accurate transcript of my stenographic notes.

IN WITNESS WHEREOF, I have hereunto set my hand this 25th day of January 2020.

FRANK GRAY
FINANCE COMMITTEE OF THE
NASSAU COUNTY LEGISLATURE

Hearing on
Financial and Payment Security and
Controls within the Office of the Nassau
County Comptroller

Committee Membership

Howard Kopel – Chair
Vincent Muscarella – Vice Chair
Thomas McKeVitt
Rose Marie Walker

Ellen Birnbaum -Ranking
Arnold Drucker
Joshua Lafazan

AGENDA
January 22, 2020
3:00 PM

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1. | Hon. Jack Schnirman  
Comptroller  
Office of the Nassau County Comptroller |
| 2. | Nancy Stanton-Molaro  
Commissioner  
Office of Information Technology |
| 3. | PUBLIC COMMENT |