PBPA Podcast Transcript
Navigating Check Fraud:
Detection, Prevention, and Recovery Strategies
(24:04 minutes)

[00:00:00] **Sireesha:** Check fraud is one of the fastest-growing financial crimes affecting organizations today, and nonprofits are not immune. In this episode of the PBPA Podcast, we're talking about check fraud, how it happens, and what practical steps nonprofits can take to reduce their risk. Join me as I chat with attorney Kurt Lentz about fraud prevention, internal controls, and what to do if your organization becomes a target

Hello and welcome to the PBPA Podcast. In each episode of the PBPA Podcast, we explore legal questions relevant to Georgia nonprofits. I'm your host Sireesha Ghanta, Counsel and Education Director at the Pro Bono Partnership of Atlanta. PBPA strengthens our community by engaging volunteer attorneys to provide nonprofits with free business legal services. We provide numerous free resources via our website, including articles and webcasts specific to Georgia nonprofits and their business legal concerns. We also provide direct legal services to our clients. For more information on client eligibility requirements, to apply to be a client or to access our vast learning center, visit our website at pbpatl.org. Before we jump into this episode's topic, keep in mind that this podcast is general information, not legal counsel, contact your attorney for guidance on your nonprofits' specific situation.

Kurt Lentz is Counsel with the law firm of Baker Hostetler here in Atlanta. He advises clients in the financial services industry about a range of complex issues, including check fraud. He has also been a wonderful volunteer with PBPA since 2011. Thanks so much for joining me in this conversation, Kurt.

[00:02:08] **Kurt:** Thanks, Resha. Happy to be here

[00:02:11] **Sireesha:** Now, Kurt, let's start very generally. What are some common ways nonprofits might become the target for check fraud by third parties?

[00:02:23] **Kurt:** Yeah it's really the same way that anybody becomes a target of check fraud by third parties. People stealing checks out of mailboxes and changing the amounts of the check, changing the person who's supposed to be paid on the check, people stealing your physical checks ,people taking your bank account information that they might be able to find somewhere and printing checks that look like they are from you, and then writing those checks to other folks. So that'd be an instance of a forged check. But a fraudulently created check and then a forged check.

One type of check fraud that is running rampant among nonprofits right now is a scheme where a fraudulent donor will send a check to a nonprofit, and then reach out to the nonprofit and say, "Hey, I wrote that check for too much. Can you send me a refund, either by wire or check?" And the nonprofit will send the money back, and those are real funds whereas the check that the fraudster has sent is not real funds. And so by the time the nonprofit learns that the check was bad, its funds have been sent to the fraudster and probably moved off-site.

So, any kind of way that your checking account or your checks may be vulnerable to someone either stealing the information on them or stealing them physically exposes you to check fraud.

[00:03:58] **Sireesha:** Wow, there's so many creative avenues for fraudsters. So what recommendations do you have? What can nonprofits do to avoid potential third-party check fraud?

[00:04:11] **Kurt:** I think the most basic thing that a nonprofit can do to avoid check fraud is to the... is safeguard your checks. Make sure that you have controls in place who has access to your checks, who's an authorized signer on your checks and that you have the proper systems to make sure that those checks, and these are your physical checks, but they're not falling in the wrong person's hands.

If you are writing a lot of checks, if you're controlling a big budget you probably want to have some kind of hiring protocol of who you hire that is going to have control of your checks. Have rules and procedures in place, who in your organization is able to issue a check, write a check, and what the processes are going to be and ways to safeguard that. Don't, if you can help it, drop physical checks in mailboxes that are public where they can be taken and washed. Uh, use ballpoint pens when writing checks because it's harder to erase them. Some of the things that nonprofits can do are very basic, but check fraud's a very basic kind of fraud usually too.

It's getting access to, hold of a physical check and then altering it in one way or the other, right? By fra... by, by forging the account holder's name or by taking a check that the account holder has written and changing the amount or changing the payee.

These are all things that you can do on the front end. Keep your checks safe, keep them locked up. Know who's writing your checks. Have processes and procedures in place for how checks go out the door. Be mindful of where you actually put your checks when you're sending them. Or these are, easy things you can do on the front end to avoid check fraud on the back end.

[00:06:00] **Sireesha:** And then what about after the checks have gone out? Is there anything that a nonprofit should be doing to monitor the checks and the deposits against their account?

[00:06:13] **Kurt:** Yeah I think one of the most important things that any nonprofit or anybody who owns a bank account can do if they're writing checks out of it, is to monitor their monthly statement. And the reason I say that is because banks operate based on when you receive your monthly statement in terms of dealing with potential check fraud issues.

And that ties back to provisions that are pretty uniform across bank deposit agreements that shorten the time for you to alert the bank of certain issues related to checks if you don't find it within X number of days from seeing it on your statement. So know what's on your statement. Even better than knowing what's on your statement is perhaps have, if you have a CFO or a controller or somebody else who is able to take even more regular stock of what's happening in your bank account. And so, you know, if you write that check for $1,000 and you see it get cashed for $10,000, someone can raise the flag right away and alert somebody to the fact that there's fraud.

Or if you see a check for $1,000 that wasn't written and wasn't expected to be written, that is out there. Um, and then when you discover if you discover that anything has happened reach out to your bank immediately. If you see it on your statement, if it looks strange, if you didn't write the check, if the check is different than the amount that it was written the most important thing that you can do is alert your bank.

And once you do that, once you're working with their fraud department or their customer accounts department they will walk you through the steps that you'll need to take to make sure that there's not further fraud and to help you get reimbursed for any checks that were cashed on your account that were not authorized.

[00:08:07] **Sireesha:** Okay. So if a nonprofit sees something suspicious or looks like there's been a fraudulent check cashed on their account, they should notify their bank, like you said, and then the bank will guide them to help give them tips on how to avoid further fraud?

[00:08:22] **Kurt:** It's most likely. I'm thinking times when I've had fraud issues on various accounts and I reach out to a bank, usually they shut down the account. They may stop payments on future checks. They may ask you, if anybody else has access to your checks. They may ask you if you want to close that account and open a new account that doesn't have the same sort of compromise issues. There's going to be someone at your bank that will be able to help you navigate the best ways to cut off any future fraudulent check issues.

And I think if you use your bank as an ally going through that process, obviously staying vigilant on, on your own end but working with them to make sure that it doesn't happen again I think there's very few banks that would not be receptive to and prepared to help you navigate that. Because while these types of check fraud issues may be a one-off instance for a nonprofit or for anybody experiencing them, banks deal in this space on a daily basis. They have a playbook where folks who are experiencing check fraud do not.

[00:09:31] **Sireesha:** That's right. And we have had situations where nonprofits who have gone through this, after they notified their bank, they have also been encouraged to reach out to their local police or even the GBI, depending on the situation.

[00:09:46] **Kurt:** Absolutely. I think and that's one thing that banks will probably ask that you do as they prepare their internal files on this, but it's something that you should do anyways, right? Because if you have a bad actor who is within your organization and is doing it that is something that you wanna know. If you have a bad actor who is targeting your organization that is something that law enforcement should know, and you can, you can suss those things out and have the record of it.

But absolutely, you should reach out to local law enforcement and it could be... I mean, depending on how the fraud occurs, you could be working with your local police, you could be working with the GBI, you could be working with the FBI, you could be working with the Secret Service. It's a sort of tangled web and a lot of it depends on how the fraud is perpetrated. But once you reach out, you don't have to know the right organization to go to on the front end. Once you reach out to one law enforcement agency if it's not their jurisdiction they will gladly keep their plate clean of that and send it to the right person to help you.

[00:10:48] **Sireesha:** And Kurt, now what if we have a situation where an organization a nonprofit, if they have a fraudulent check and the bank cashes the fraudulent check, and then the bank is not able to reimburse them. Can you walk us through that?

[00:11:06] **Kurt:** Yeah. So if the if there's a, if there's a fraudulent check that the bank's not able to reimburse you for, what it's going to boil down to is something happened in the various warranties that all banks...

So when you write a check it goes to someone, or even a fraudulent check. Somebody has a check, they try to deposit it at a bank. That bank will present it to another bank to get the funds. And this is all done on a back end through various other third parties. And every time a bank makes a, every time a bank presents that check to another bank to settle those funds there's certain warranties that are made.

And a breach of those warranties is how it's determined who's going to ultimately be liable for a check. So if it's a forged situation, so someone has taken a check or created a check and forged your signature. Typically unless you have let, left your checkbook out somewhere or made your checking information available somewhere where your bank can say that you were negligent they will reimburse you for those funds.

Now, if you haven't safeguarded your checking account information, if you haven't acted reasonably to make sure that the fraud hadn't occurred then that's going to affect certain defenses that your bank has and that the presenting banks have in these warranty breach situations. So if they can point to you and say you haven't protected your checking information the way you're supposed to, that's when you're going to end up not getting reimbursement from the bank.

Where you can find that is by looking at your deposit agreement. I worked at a bank for several years. I haven't opened a ton of bank accounts. I have bank accounts. I doubt I've ever read a deposit agreement. But having worked at banks and dealt with these issues I know that if you have a check issue and you're trying to get reimbursed, the bank is going to look directly at the deposit agreement that you were given an opportunity... you were given a copy of most likely when you opened the account or you were pointed to it. But you almost certainly would have signed a signature card for the bank that says, "Hey, I've looked at the deposit agreement. I agree to all of its terms." And that's all the law really requires on any agreement that you sign.

And so that agreement most likely has in it provisions on what it means to reasonably safeguard your account, how much time you have to alert the bank to these issues. And if you follow what is in the deposit agreement for a fraudulent check issue, you're most likely going to be reimbursed. Checks, even though they are widely abused in fraudulent schemes banks more often than not, end up bearing the loss.

Whether it's your bank or the bank where the check was deposited by the fraudster the laws around fraudulent checks are more friendly than they are for, say, wires. But if you do what is in the deposit agreement, both in terms of safeguarding your account information, safeguarding your checks alerting the bank timely to any issues that you see on your statement, or like I said earlier, if you can find it before your statement arrives, that's even better, right?

As soon as you see something, say something. You should be able, in most circumstances to avoid bearing the loss of any check fraud issues.

[00:15:02] **Sireesha:** So it's important for nonprofits to set up a system to identify dubious checks quickly, and if you do notice suspicious check activity, immediately notify your bank. You don't want to wait long because then you could have multiple bad checks coming through, and you don't cash che- until multiple bad checks have gone through. And you should have someone within the organization who is different from the person who is writing the checks to do that double checking. Because if the bad actor is the person who is writing the check, and they are also the one who is checking the account, then that's not gonna be caught.

So try to have more than one person involved in that process.

So far we have talked about check fraud. But I wanted to ask briefly if there is any other advice or guidance related to ACH or wire fraud. You briefly mentioned wire fraud just now. Any guidance for organizations to avoid or navigate ACH or wire fraud?

[00:16:08] **Kurt:** Yeah. Wire fraud in particular most people have probably seen or read an article about a scheme called BEC, business email compromise. And it is a multi-billion dollar fraudulent scheme, and it works by bad actors infiltrating your email system or one of your vendor's email systems and they sit in there and they lurk and they wait until they see that there's going to be a payment, and then they start interacting with you and manipulating your emails of what you see and what goes out so that at the end of the day, what happens is they give you bad wire instructions, and you end up wiring the funds to a bad account.

And now, that is an issue because, going back to this idea of what your agreement with your bank says the agreement on wire transfers at your bank probably says something along the lines of, "If you give us if you give us instructions, even if they don't end up being the instructions that you thought they were or you wanted them to be, our responsibility ends when that wire goes out."

And so wire fraud, unlike check fraud, is an issue where the customer, the nonprofit, would more likely end up bearing the loss than the bank. Um, because once it goes out, your bank isn't going to reimburse you, and the bank who received the funds is not... they will send back any funds that they're still holding. Banks have this system where they work together to return fraudulent funds that they might still be holding. But if they're not holding them or if they're only holding a part of them, that's what you're going to get back. And the unfortunate part of this is international banks do not participate in this kind of sending the money back. So as soon as you wire those funds from bank A to bank B, your fraudster at bank B is going to wire them to bank accounts overseas almost immediately. So you have a very quick window of time to fix that. And unfortunately, most people or many people when they're involved in that will not will not stop that.

If you're sending a wire, or expecting to receive a wire you can't be vigilant enough in picking up the phone calling your known contact, your donor, your vendor, whatever the case may be saying, "Hey, just wanna make sure that this, these are the wire instructions we're using."

Um, don't call people back on phone numbers that may have changed. If you have a CRM system that- has and tracks what your donor's information is use that. Don't use what someone sends you in an email. Be careful of folks emailing from an email addresses you haven't seen.

And, and unfortunately there, there's ways to mask all of this for fraudsters around wires and make it very hard. So, you know, they might change in an email address like a Q to a P. Like little small things, right? That you just don't know or to look for. And then the way it inevitably plays out is, is the person who is expecting to receive money will call you a couple of days later and say, "Hey, you know, that wire you were going to send never came in."

Or they'll call you, "Hey, did you get that wire that I tried to send?" And the answer is no, and by that time, unfortunately, it's usually too late. Be hypervigilant around any strangeness around either sending a wire out to somebody and my guess is that nonprofits are probably more likely to be receiving a wire.

It would be a potential donor who's, maybe losing funds, but even then, that's not going to be it's not gonna be a good day for the donor and not a good day for the nonprofit. Anything around wires y- I- I just don't think there's enough caution that people can exercise around those. And, for those, you should probably have some sort of internal policy and procedure in place of how are we going ... how are we, the nonprofit, going to confirm that the right instructions are being sent to our customers, or if we're sending wires, how are we gonna make sure that things are going to the right recipients? Because like you said, once it's once the money's been sent, it is very hard to get back.

And that is one where you need to if you do have a wire fraud incident loop in law enforcement right away, and it... that one is going to be probably FBI and Secret Service. It's going to be federal law enforcement agencies who are dealing with that primarily due to the interstate nature of it.

[00:21:23] **Sireesha:** I agree with you, Kurt. I don't think it's very often that our nonprofits are sending wires. It's more often that they're receiving them. But it's very helpful to have this background on wire fraud and how it might happen and how it plays differently than check fraud. For my last question to wrap up, if there's one takeaway you want for our nonprofits listeners to hold onto, what would that be?

[00:21:53] **Kurt:** Be very vigilant. Um, know who can write checks, know where you might have any vulnerabilities and remove them. And then be vigilant in monitoring your accounts. Don't let something go more than 90 days after you receive a statement, or really 60 days or 30 days. If you see something, say something, and say it immediately.

Call your bank. Every bank has a fraud hotline that you can call. It's probably in your deposit agreement which you can find. Most of banks' deposit agreements you don't have it laying around probably, but you can Google your bank's name and deposit agreement and find that information. Let your bank know as soon as possible if something does happen. Do as much as you can on the front end to make sure that you've got the right people in place and the right processes in place to make sure that you don't have forged or fraudulent checks going out on the front end.

[00:22:59] **Sireesha:** This has been so much good information, Kurt. Not just good background, but good practical tips for nonprofits to try to help them avoid check fraud instances, and then if they do have one, steps that they can take.

Thank you so much for sharing your time and expertise with us today.

[00:23:17] **Kurt:** Oh, thank you for having me.

[00:23:22] **Sireesha:** We hope that you found this episode of the PBPA Podcast to be informative and helpful. We add new episodes every month with short conversations about general, yet important legal information for Georgia nonprofits. Remember that this is not legal counsel. Talk to your attorney about your organization's specific concerns. Thanks for tuning into the PBPA Podcast. And to all nonprofits listening out there, thank you for all the good work you continue to do in our community.