PBPA Podcast Transcript
Episode 29 – Protecting Your Nonprofit from Scams, Fraud & Imposters
(34:59 minutes)

Sireesha (00:03):

Nonprofits of all types are susceptible to fraud, especially those with limited resources and internal controls. Nonprofits also exist based on strong brand reputation—meaning a fraud event could be devastating. What should you do if your nonprofit is the victim of a scam or fraud? In this episode of the PBPA podcast, we will be talking to Noula Zaharis, Director of Securities and Charities Division with the Georgia Secretary of State, and Anna Burns, the Regional Director of the Federal Trade Commission's Southeast Regional Office. Anna and Noula will draw from their extensive experience to talk to us about practical steps nonprofits can take to protect themselves against fraud.

Sireesha (00:58):

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.

Sireesha (02:09):

Anna, Noula. Thank you so much for joining us today.

Anna (02:13):

Thank you for having me.

Noula (02:15):

Yes. Thank you for having me too.

Sireesha (02:18):

So today we have guests from the Georgia Secretary of State and the Federal Trade Commission. To start off, can you clarify, why are the secretary of state and FTC involved in this topic?

Anna (02:31):

The Federal Trade Commission's mission is to protect the American public from unfair or deceptive acts or practices in the marketplace, meaning that we fight frauds, educate others about frauds and bring enforcement actions regarding frauds that affect the American public.

Noula (02:51):

For the Georgia Secretary of State, we have found that charity fraud is an epidemic that has swept across the world and specifically the United States recently. So, the Georgia Secretary of State

proactively engages in outreach programs like the one that we're doing today in order to work with both the donor and the charity on how to safeguard yourselves from being a victim of fraud. The Georgia secretary of state is responsible for regulating various industries on the state level, including charities. So fundraising activities are regulated by state law. The Georgia charitable solicitation act governs the registration, the reporting, and the enforcement of fundraising activities within Georgia. And the duty of our division, the charities division, is to enforce the laws regulating the charities, the paid solicitors, who are for-profit companies that charities contract with to raise money, and these solicitor agents who are individuals who work for those companies that, you know, raise money.

Noula (03:58):

And then we also are here to ensure the proper administration of funds dedicated to charitable purposes. One thing that we have found in our division is that a lot of charities confuse our division with the Corporations Division. So, whether or not your charity is formed, you know, under the laws of the state of Georgia, it must be registered to conduct business in the state. So, registering your charity as a domestic corporation or a foreign corporation in order to do business in Georgia is done through the Corporations Division. However, there's one more step. And that step is to register with our division. Charities that solicit or accept donations from Georgia are also required to register with our division in order to do that fundraising and to do that solicitation. So, our division also has a duty to protect donors from financial exploitation.

Noula (04:55):

However, in recent years, we've seen that the charitable organizations themselves are becoming victims of fraud. You know, as I said earlier, that charities fraud is an epidemic, and there are two types. There is the internal fraud, which is committed by someone within your organization, or someone connected to the charity. And then there's the external fraud, which is committed by someone with no connection to the charity at all. So we recently are seeing an uptick on the external fraud complaints. This is when someone knowingly impersonates a charity in order to deceive people into donating to this fake charity. They can do this by creating an organization that has a name very, very similar to the legitimate charity's name and pretending to be a legitimate charity, or by pretending to be you—your charity. I call it, you know, charity identity theft.

Anna (05:52):

To build off what Noula said, where she was talking about a rise of fraud reported her organization, the FTC also has seen a rise in complaints regarding fraud and imposter theft. For example, in 2021, we received reports of $5.8 billion lost to fraudulent schemes at the FTC, which was a 70% increase over 2020. With that we had 5.7 million actual reports and 2.8 million of those were fraud reports. And so this is an increasing problem, and so the best way for charities to protect themselves is to be aware of what is going on so that they can both take proactive steps to protect their charity from fraud, as well as know where to report it if fraud happens, right.

Sireesha (06:46):

A nonprofit may not know what to look out for if it's been fortunate enough to have a never experienced fraud. Can you provide some general examples of fraud that have happened to charities?

Noula (06:59):

I'll go first. For Georgia, so we've seen—this is very timely because we're actually in the process of investigating three broad complaints involving, you know, kind of an identity theft of the charity. The first one involves phishing and false websites, like other frauds, fraudulent charities also utilize phishing schemes to defraud donors. A recent scheme that we're looking into involved a fraudster who copied a local legitimate charity's branding, social media, and logos. The fraudster created similar, and in some cases identical, social media posts or emails, soliciting donations, and other personal information. The victims then clicked on the hyperlinks that were associated with those social media posts or emails. And instead of being transported to the legitimate charity's website, they were sent to a fraudulent site where their personal information was collected and sent to the bad actors. And we, this is frequently seen on social media and via email campaigns.

Noula (08:03):

So in these types of frauds or scenarios, not all the fraudsters are actually soliciting for donations. In this instance, the fraudster was phishing for social security numbers, dates of birth, bank account information, driver's license information, and other personal identifying information, which then they used to commit identity theft. A second one that we're looking into involves a vendor fraud. A local charity recently discovered that bad actors were purchasing expensive equipment in the charity's name. So the bad actors submitted purchase orders to the vendors in the name of the legitimate charity. The equipment was delivered to the bad actor and the legitimate charity was sent the invoice for the items that they never ordered nor received. So the bad actors accomplished this by targeting charities with generic names and making subtle changes when they create an organization.

Noula (09:08):

For example, let's say there's the Noula Zaharis Nonprofit Corporation, which is a legitimate charity. And the fraudster goes in and creates on a corporation site, no matter what state the Noula Zaharis Association, and pretty much copies, you know, my website and everything. And the bad actors use these names, also use the names of dissolved corporations so that if a vendor were to go search them, you know, to see who this entity is, they would receive search results for the legitimate charity and also for the dissolved corporation, muddying the waters and making it difficult to discern fact from fraud. So that's our second one. And then our third one, which I found the most interesting, was using a false affiliation or partnership. There are some bad actors out there that will bolster their credibility by telling potential donors that they are partnered with legitimate, more recognizable charities.

Noula (10:05):

The bad actors are not necessarily telling people that they themselves are legitimate charities. Instead, they use ambiguous terms such as, "Oh, I've partnered with Noula's nonprofit and I'm working with Noula's nonprofit". So, the division recently saw this happen when a nonprofit corporation that was registered with the Corporations Division was soliciting donations door to door. They would tell donors that they were partnered with a legitimate and well-known local charity in order to gain credibility and increase the likelihood of collecting money. We were made aware of this scheme when the bad actor knocked on the door of the legitimate local charities, board member. And so, the bad actor told the board member that he had partnered with the board member's own charity. The board member, recognizing that this was a misrepresentation, politely listened, gathered all the information, and called us to report it. So those are the three that we've looked into recently.

Sireesha (11:07):

Those are, they sound like such crazy stories, but—

Noula
Yes.

Sireesha
They are real life.

Noula
Real life.

Anna (11:13):
Like Noula, the Federal Trade Commission has seen a rise in imposter scams, and as Noula was explaining, those imposter scams can take many forms. So, one would be somebody pretending to be the charity itself and soliciting donations on your behalf, ultimately harming your reputation with donors and with the outside community, but charities like any small business could also fall victim to imposter scams with people who are pretending to be, for example, a vendor or somebody within the organization itself and taking money or information from the charity that way. So, for example, one type of scam that often happens with small businesses—and charities are no exception—is a business email compromise scam. So this is when somebody pretends to be someone within your organization, creates an email address that looks very similar or is identical in many cases because they've hacked into your system, and they email other employees in your organization, either asking for money or asking for information that would otherwise be private.

Anna (12:23):
So for example, one report that we received here in Georgia was a young member of a nonprofit was instructed by email from a senior member to buy gift cards. It was the holidays said, you know, we're giving gift cards to people without the means to purchase gifts themselves or for gifts with for people in the organization itself. And so go to your local drug store and I need you to buy thousands of dollars' worth of gift cards, because we're going to be handing these out at the holidays and use your purchase card. So, the employee went purchased the gift cards and then got back to the office and received another email saying, hey, send me the numbers off the back of the gift cards because we need, you know, I'm not going be able to distribute these; I have a sick family members. We're just going to give people the number so that they can shop online. The employee did that and then got another email a couple of days later saying, hey, you did a great job. And you know, he's thinking this all is coming from his boss. You did a great job. I need you to go out and do this again. And he went to the same drug store and the employee at the drug store—at the cash register actually—said, sweetheart, I think that you are being victimized here. But he said, no, no, no. I have an email from my boss telling me to do this, so actually went to another drug store and purchased thousands of dollars more of gift cards before he realized while he was leaving that drug store, I think that I am—there's something not right about this.

Anna (14:03):
So then he realized he'd fallen victim of a fraud. And you know, this story sounds like why didn't this employee realize, but this happens all the time. You receive an email from your superior, you are told

it's an emergency, you know, and you're trying to do the best job that you can. And so fraudsters are sophisticated. They know, you know, how to prey on people. They know what to ask. They know what to say in order to get you to do what, you know, they want you to do. And so that they can take the money. And in this case with gift cards, that money is gone, as soon as those numbers are read off the back.

Anna (14:55):

Other scams that we've seen are invoice scams. So, for example, people will receive an invoice to their nonprofit or to their small business. And it'll be for example, a yellow pages invoice saying you owe X number of dollars for your ad in the yellow pages. And you know, it will have the logo of the yellow pages on there, which is not trademarked. And they will just assume it's their legitimate ad or it's their legitimate listing, or online ad. And they'll pay it. And this could go on for months and months because people don't question it. They think that they're just doing their job, paying these invoices. And another one of those is search engine optimization. We have seen has grown with these invoice scams as well because more people are advertising on the internet than they are say in a traditional phone book these days. So there these things that you wouldn't think of because they just seem so rote, they don't seem like something that you would question, but there are things to be on the lookout for. And so the best way to avoid these types of scams is to know about them and train your employees to be on the lookout for them.

Sireesha (16:04):

These examples are very illuminating. And we'll talk a little bit more later about steps nonprofits can take as they become more aware of these possibilities. But I wanted to ask about one concern that nonprofits always have is they want to ensure that the funds that donors are giving, that are intended for the legitimate nonprofit are actually going to them. But sometimes that can be easier said than done, especially when it comes to technology. Noula, do you have any specific suggestions to help nonprofits make sure that the funds that are intended to them actually come to them?

Noula (16:47):

Yes. And let me stop here and say that the views that I'm about to express do not necessarily reflect the views of the secretary of state. But in our outreach, the Georgia Secretary of State does a lot of outreach to donors. And one thing that we keep telling donors is to make sure you know where your money's going and how much of that money's going there. So we're telling, we're starting to tell charities the same thing, and these are some things that, from what we've seen, that we would suggest, you know, that the charities think about. First, it's important to educate your donors, especially about how you solicit. I really feel very strongly about education and educating, you know, the consumer. So, educate your donors. Explicitly tell your donors what type of solicitation your charity does and does not do. For example, the Noula Zaharis Nonprofit does not solicit door to door.

Noula (17:42):

You know, if you receive door to door solicitations claiming to be associated with Noula Zaharis Nonprofit, report that to us or report it to, you know, to the Charities Division at the Georgia Secretary of State. We really feel that it is important to educate your donors. You need to beef up the disclosures on your website and your transparency to your donors about how you solicit your funds, how you fundraise. Do you use third party companies, those paid solicitors? And if so, maybe think about listing who you use on your website. So that when I get the call as a donor, you know, I'm going to recognize

that or I'm going to go look it up and say, oh yes, they do have a partnership. Are you on a list of charities that uses online retailers, social media hubs, crowdfunding sites, or other such portals? Do you send people door to door?

Noula (18:36):

You know, have you partnered with other organizations? Like the gentleman who went to the board member, you know, and if you have partnered them, think about putting that on your website. Believe it or not, there's some bad charities out there that say they accept cryptocurrency gift cards and cash. Do you do that or do you never do that? You know, just be very explicit as possible on the website to educate the donor. And you might want to take an extra step and remind your donors that is important for your donors to utilize the same phish-prevention techniques that they would apply to their emails, you know, to apply those techniques, to even social media posts as well. Because, you know, that's where, you know, the one with the first one I told you where it was the imposter, they took over the website and the social media, you know, just make sure that they're not being phished for to get their personal information.

Noula (19:34):

Another suggestion that we have is to link your charity's page to a credible third party site, such as check Charity Navigator. You know, we encourage donors when we do outreach to check out charities before they make donations. And we encourage them to check the watchdogs like Charity Navigator, Charity Watch, the Better Business Bureau's Wise Giving Alliance. And those agencies not only rate the organization, but sometimes provide access to your 990s. Our suggestion is to make sure you have a presence on those sites, so that, you know, the donors can go and feel comfortable if they see you there. A third suggestion is to provide proof of your nonprofit status. Like maybe on your website show that you are a registered 501(c)(3) organization. You can do this by putting a link to the IRS website. The IRS has a tool called IRS search for tax exempt organizations.

Noula (20:37):

You don't necessarily, when you search that site, need to put an EIN number as part of that search. The name of the charity is good enough, and what's great about that is if you put the name in, it'll pop up all the various names that are similar sounding, you know, to your charity name. So you'll see, you know, you may seem more than like, yeah, you may see Noula Zaharis Nonprofit, LLC, and Noula Zaharis Nonprofit Association. I personally, you know, would not be giving out my EIN number. I can tell you that our division is very protective of the charity information that you provide us when you do your registration. So, when we get open records requests asking for documents that charities have submitted as part of the registration, we are very mindful of redacting very sensitive information, which includes your EIN number, your addresses and telephone numbers of board members and officers, and even donors.

Noula (21:41):

You know, we go through those documents and make sure that whatever we send out, it does not compromise, you know, the charity at all. The fourth thing I would highly suggest is to monitor your corporate filings. There is a lot of corporate identity theft. This is where the fraudster will attempt to have open lines of credit in the name of the established corporate entity. A typical scenario that we're seeing is that a bad actor goes into the corporation site and files an amendment on your behalf. Now in Georgia, we have millions of corporations that are organized here in Georgia, and then there's a difficult

task to monitor every filing that is made on our end. So as a business owner, you need to be very vigilant and proactive in monitoring your corporate filings, no matter what state they're in. We recommend that you monitor those corporate filings, check in where your accounts are held, and better safe and sorry, change login credentials frequently. Treat it like this is your bank account, or like a stolen credit card. Go approach it with that way.

Noula (22:53):

More importantly, if you suspect that your business has been compromised, that you need to call our division and/or the FTC and/or law enforcement. And then the final thing that we would recommend is that you need to ensure that your website isn't duplicated and the best way to do that is probably to schedule routine times to Google your nonprofit and search your nonprofit and social media and see what's out there. So those are some steps that we would say to take into consideration.

Sireesha (23:26):

Wow, that's some really good, practical information.

Anna (23:30):

Just to add to what Noula said, and she covered so much of it, but make sure if you're dealing with technology that your own internal technology, that your systems are up to date, and that you are doing everything you can to protect those systems from outside hackers or from people within your organization who shouldn't have information that they don't otherwise need. So, for example, one thing that we see is, you know, when people lose money, is that internally that their passwords aren't protected, that they are leaving their system vulnerable to fraud because they're not doing the required system updates. It's very easy just to click off of, you know, this security tool needs updates. Like, would you like to do this now? Or do you like to do this in an hour, make sure that you and your employees are actually doing it now because without those updates, your system is otherwise vulnerable to people from outside and within your organization. And just to follow up on that, make sure that you have internal processes and procedures in place for people to follow when it comes to using technology so that they know what information they can share on social media, what information should be on your website and make sure that, as Noula is saying, that your website is protected from external forces.

Sireesha (24:59):

Yeah. That, you know, nonprofits can be defrauded by people outside their organization and, as you mentioned, inside their organization. Do you have any suggestions for other steps nonprofits can take to minimize the risk of fraud from within their organization?

Anna (25:18):

I think one of the most important steps that people can take to protect themselves from fraud with inside their own organization is training. Make sure that your employees are trained so that they can spot fraud if it's occurring with others. Make sure that you yourself are trained. If you're leading an organization to know what to look out for. One of the most difficult things that we all experience is that a lot of the times we think that fraud happens from unknown external actors, but a lot of times fraud happens from our acquaintances, employees, trusted, loved ones. And so, we really need to make sure that information is protected. So, one thing we say is if somebody doesn't need access to certain information, you know, don't allow them to have it. So don't allow people who don't need access to bank account information to have it, or access to your IT system or access to your donor lists because

one thing that is particularly vulnerable is not just money, but it's information and data that is kept internally. And make sure that you're protecting, you know, that data by keeping it in secure programs. And, for example, you shouldn't be keeping people's bank account information unless they've given you permission to do so, but if you are, you need to make, and then double check to make sure that that information is secure.

Noula (26:47):

Yes. And I'll add to that again, you know, to kind of reiterate that it's very important to make sure that you have cybersecurity measures in place. Regularly update your protection software, as well as protecting your devices, using antivirus software. Your staff and your volunteers should be made aware of any potential email scams and how to avoid them. I think it's also, in this day and age, probably good to think about establishing a fraud prevention policy. This can help raise awareness of fraud risks, as well as help your staff and volunteers take appropriate steps to prevent, detect and act if there is fraud. You might want to have a plan for how your charity will respond to that fraud. You know, who in the charity needs to be told, and it who, if anyone outside the charity needs to be informed. As Anna said, you know, you should implement sound financial internal controls to safeguard your data, you know, regularly check your charity's accounts and records.

Noula (27:46):

Also, people commit fraud for a variety of reasons: to pay debts, maybe out of greed, or through opportunism. You know, that doesn't happen just externally, but it can happen internally. So, it would be wise to be alert to behavior changes of any of those in your charities, such as, you know, board member, committee, member, staff, or volunteers. Be alert to things like that. If you are hiring a third-party professional to do your fundraising, make sure that you vet that company before you have that contract in place. And before you start sharing data. Many charities as many of you know, use third-party for-profit companies to solicit donations for the charity itself. And many of you may not know that this activity also requires registration in Georgia, meaning that the third-party for-profit entity must register it with our division as a paid solicitor.

Noula (28:46):

And as part of that registration, the for-profit paid solicitor must provide the contract it has with the charity to our division. And that contract must show the duration of the campaign and the percentage that the paid solicitor will keep from the campaign raised. And then at the end of that campaign, that paid solicitor must provide to the Charities Division a financial report, detailing the amount raised, the amount that went to the charity, and the amount that that paid solicitor kept. In our outreach to donors, we encourage our donors to ask the caller if they work directly with the charity or if they're part of this third-party fundraiser. So, if you're engaging a third-party for-profit company to act as a paid solicitor, we would encourage you to reach out to us to see if they're registered. I will tell you that currently we have 90 such firms registered in Georgia with us.

Noula (29:41):

And the reason why I'm encouraging you to reach out to us is because of an incident that happened this past year. We had a fraudster pretend to be a paid solicitor. He was actually impersonating a legit paid solicitor that was registered with our division. He created a company named very similar, almost identical to the legit paid solicitor. He actually went as far as hiring call center agents to make calls to donors, asking for money for the legit charities, but the monies were not going to the charities nor to

the legit paid solicitor. They were actually going to be fraudster's personal PayPal account. On one such call, one of the donors asked the agent the question, well, how much are you keeping? And how much is the charity keeping? And the agent didn't know the answer to that question. So instead of calling the number that the fraudster told her to call, should she have any questions when she had issues with calls, she Googled to check the paid solicitor, and found the legit paid solicitor's website, called that number only to find out that they didn't know who she was, she didn't work for them, and in that conversation, they were able to get enough information about the entire scheme so that our division and other state officials and law enforcement stopped him from that. So, it's important to check out and vet your vendors.

Anna (31:05):

And as Noula was talking about third-party vendors, one thing that you want to make sure to include in those contracts is cybersecurity measures. So whatever measures you're taking to protect your own charity, you want to make sure that they are equally protecting the information that you don't want made public. Donors care about the privacy of their personal information and savvy businesses and charities understand the importance of being clear about what you do with their data too. So, also make sure that you're telling your donors what you're doing with their data, either on your website when you're collecting it, and make sure that your third party vendors are as well.

Sireesha (31:47):

You guys brought up so many great points here. I am going to include some links to charitable registration and working with solicitors so that if any listeners need more information on that they can find those resources on our website.

Noula (32:04):

I do want to add one thing you said about resources. So, on our website—the Georgia Secretary of State's website—we have a section called Resources for Businesses on our charity page. But on that page, we have links to four wonderful resources that were developed by the FTC. And those four really speak to charities. One is called Online Charity Giving Portals: Tips for Retailers, How to Review Charity Requests: Start with Security, A Guide for Business, and then Raising Funds: Hiring a Professional. Those are very good resources. And we have links, to the FTC site. And finally, I want to reiterate that if you really suspect your charity has been compromised, like call us, call our division at the Georgia Secretary of State, call the FTC, call the law enforcement. That is what we're here for: to protect you the legitimate charity, as well as your donors

Anna (33:03):

Nuola. You beat me to mentioning those.

Noula (33:05):

Yeah. I'm sorry. You've got references.

Anna (33:07):

No, it's great. We obviously think that those resources are great, too. Yes. And please utilize them and please send them to others, too. If you have friends who are in charitable organizations, if you're in organizations that have others with similar needs, we encourage you to share them as well.

Sireesha (33:27):

Great. And we will include links, those four links, on the podcast episode page. So, listeners can easily access those. But thank you, Anna and Noula, for taking the time today to speak with us. This was very eye opening. You know, this information will allow nonprofits to understand the risks that you have discussed and help them to know what necessary preventive measures to take so that the nonprofits can reduce the potential for fraud, which comes in many forms as we've learned today. Thank you, Anna. Thank you, Noula so much for joining us in this conversation.

Anna (34:03):

Thank you. It was a pleasure to be here.

Noula (34:04):

Thank you for having us.

Sireesha (34:07):

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.