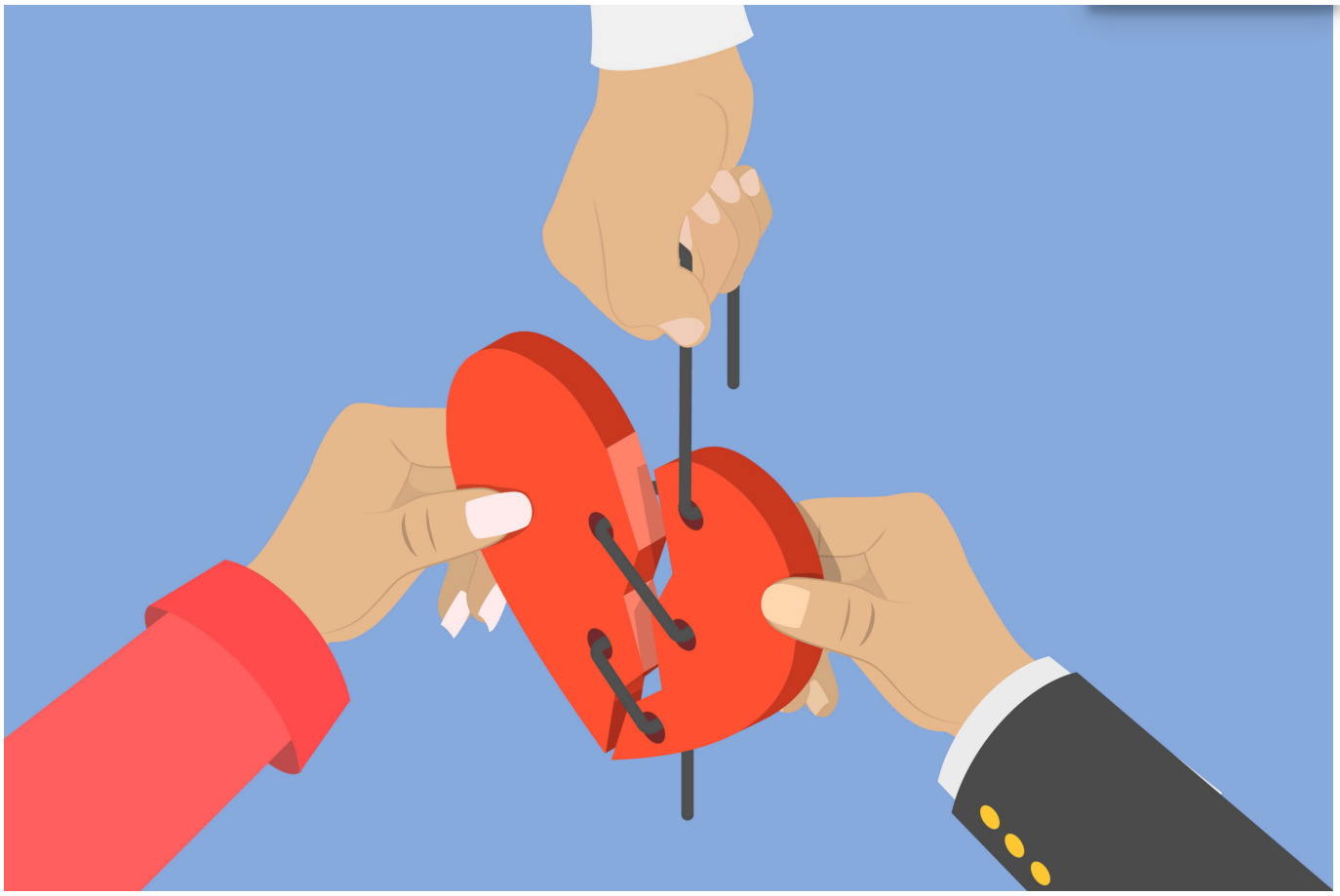
SOLUTIONS

After Donor Data Is Compromised, How to Restore Trust

A data breach can damage fundraising for years. Here's how to regain trust through honest communication, proactive updates, and consistent security.

By **Rasheeda Childress**
Senior Editor, Fundraising



Getty Images

January 28, 2026 | Read Time: 7 minutes

In November Princeton University's donor database was breached, exposing email addresses, phone numbers, street addresses, and information about donations. That was less than a month after those claiming responsibility for a breach at the University of Pennsylvania released thousands of files including memos about donors. Large nonprofits including Catholic Charities divisions and the Salvation Army, have also experienced data losses.

It is clear that hackers know that nonprofits keep troves of data on their donors that has great value. And though attacks are more common, that doesn't make them any less traumatic for those affected. These breaches can quickly undermine trust in the organization, which can dampen fundraising, say experts.

But even in the face of such a public failure that affects such a sensitive and important group as its supporters, there is a lot that organizations can do to mitigate the damage and rebuild relationships with their donors. Princeton declined to discuss its data breach or the methods it is using to rebuild trust, but several experts told the *Chronicle* that nonprofits can recover through transparency, targeted messaging, and building a new track record of care.

The Reputational Harm of Donor Database

Data breaches have increased in frequency in recent years, reaching more than 3,100 incidents and resulting in 1.3 billion breach notices sent to consumers in 2024 — the most recent year for which data is available.

However, just because people are hearing about these incidents more often, doesn't mean they care any less when it happens to them. The BBB Wise Giving Alliance surveyed charity donors about trust in their 2025 Give.org Donor Trust Special Report. Twenty-eight percent of those surveyed said they would not donate to a nonprofit again if their data had been stolen from the group. A larger number, 52 percent, said they would hold off donating until they were satisfied the issue had been resolved.

"There is a significant number that would stop giving if they hear about a breach," says Bennett Weiner, CEO of the BBB Wise Giving Alliance.

And while a specific length of time donors held a breach against nonprofits wasn't available in the Donor Trust survey, there are lessons from the for-profit world, says Christoph Schiller, an author of the research "Hacking Corporate Reputations." The 2024 paper examined the impact of data breaches on corporate reputations and the efforts they took to repair harm and rebuild trust.

In his research, Schiller found companies that experienced a data breach performed worse than those that had not for as long as four years after the event. Those findings should also be applicable to nonprofits, says Schiller. "We find that this is not just a short-term thing," he says.

First Steps in Rebuilding Trust

Given the long-term impact that breaches can have on donors' trust of the organization and their desire to give, groups need to work quickly to rebuild trust. Depending on the state a nonprofit is located in, one of the first steps organizations take may be dictated by law — 20 states have consumer data privacy laws

"The number-one thing you have to do is follow the regulations," Weiner says. "And if the data is across multiple states, you're going to follow the regulations of more than just one."

Next up, give a sincere and genuine apology, says Lynne Wester, founder of Donor Relations Group, a fundraising consulting firm. Often, she notes, organizations will try to shift blame to vendors or others when really they need to "just come out and say, We made a mistake."

While it's important to follow the legal requirements, Wester says, it's helpful to speak plainly when sharing what happened and your intentions moving forward. "Data breach commentary is stilted — it's full of legalese," she says. "But nonprofits and giving are all about human relationships. So we need to distill that and make it clear."

In addition to the apology, it's important to be transparent about what went wrong and how it will be fixed. "The openness of what actions you're taking is a key component to regaining trust," says Weiner.

Target Messaging, Pay Attention to Media

Corporations tend to get bad headlines over data breaches more often than nonprofits and have greater resources to address the problems so their responses can be instructive, says Schiller, the researcher. The first is that corporations target their messaging to those most affected by the breach. For example, if employees were impacted, they often raised salaries. When local community members were impacted, they focused on doing good locally, even giving to local charities.

"They are tailoring their responses to specific stakeholders where the reputation loss is the most tangible," Schiller says.

That targeted approach is important for charities, too, says Shellie Bowman, a public administration strategist who works with nonprofits.

"Have an incident response planned for your donors across the spectrum — from small to large," he says. "And don't forget about your board members and volunteers if they're affected."

Major donors may need some extra attention from frontline fundraisers, says Donor Relations Group founder Wester. "They should all be ready to have that conversation in an intelligent and compassionate manner, saying, 'I can only imagine how scary that is,'" she says. They should be available to address concerns and answer questions.

Additionally, Schiller's research found that companies rebuilding their reputation focused on getting media to cover their efforts to address the breach, as media generally spent a lot of time covering the negative impacts of the hack.

Long-Term Trust Follow-Up

There's a popular saying that "trust takes years to build, seconds to break, and forever to repair." While forever is hyperbole, it definitely takes more than a single note to rebuild trust with donors.

A common mistake nonprofits fall into is making a single statement and then going silent, Wester says.

Instead, she suggests telling the donors affected by the breach that the nonprofit will provide updates on the investigation and security upgrades. Give specific benchmarks, such as indicating that the organization will tell donors about its new system next month or will have a preliminary investigation report in six months.

"You're setting expectations and a timeline," Wester says. "Be sure to deliver on that, too. When the time comes, say, 'It's six months after our data breach. Here's what we've learned. Here's how we've become better, and here's what we're doing to protect you.'"

Part of the long-term plans and communications should include improving security. Weiner says having the right software, backups, and cybersecurity insurance are important steps, but so are "staff training" to ensure user error doesn't lead to loss.

Updating security is important to rebuilding trust with donors. Respondents in the BBB Wise Giving Alliance survey who said they would stop giving after a hack were asked what would make them trust the organization enough to give again. The top answers included updating security, sharing those updates with donors, and a third party verifying that data is secure.

After that, it's crucial to continue performing well in the months following any type of breach, adds Bowman.

If a group has a second data breach that is even worse than the first, "all bets are off the table," he says. "A donor is going to say, 'I don't trust this organization.'"

Staying engaged with donors, sharing the wins and improvements of the organization and continuing to have an environment in which the organization values and protects data will be key.

"The long-term is proved through actions, not conversations," Wester says. "It's in the way you showcase your behavior. That's what will rebuild long-term trust. You can't rely on, 'Time will just heal it and they'll forget about it eventually.' There has to be proactive mindfulness taken towards it."

Today's Top Jobs

Partnerships Manager
Myriad USA

Senior Director, Annual and Reunion Giving
Pomona College

Chief Philanthropy Officer
Hartford HealthCare

Major Gifts Officer
The Jewish Federation of Sarasota-Manatee

Executive Director
Carter Burden Network

SEE MORE JOBS

About the Author

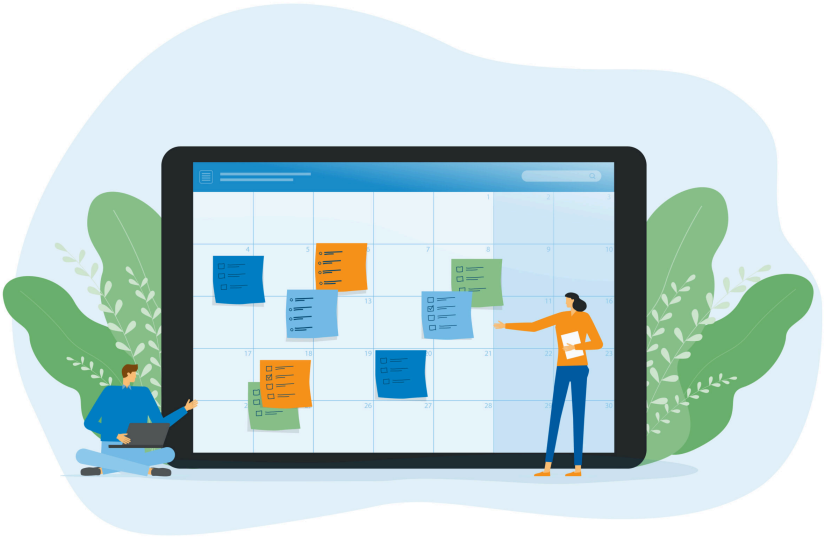
Rasheeda Childress

Senior Editor, Fundraising

Rasheeda Childress is the senior editor for fundraising at the *Chronicle of Philanthropy,* where she helps guide coverage of the field.Before joining the *Chronicle,* she covered financial and business news about nonprofit associations at *Associations Now.* Childress is a longtime journalist who has written and edited a variety of publications, including the *Kansas City Star, Higher Education Technology News,* and *Campus Crime*. She holds a bachelor's degree from Howard University in Washington, D.C.

Contact: rasheeda.childress@philanthropy.com

More Solutions



SOLUTIONS

Build a Smart Donor-Communications Plan for 2026

By LISA SCHOHL
Contributor

SOLUTIONS

Win Over Corporate Donors Amid Tax Changes

By M.J. Prest
Senior Editor, Solutions

SOLUTIONS

Conquering Turnover With Culture, Flexibility, and Growth Paths

By Rasheeda Childress
Senior Editor, Fundraising

Editor's Picks

CORPORATIONS

Why the $130 Billion OpenAI Foundation Has Other Nonprofits on Edge

OPINION

Philanthropy Must Stand Up for Minneapolis — and Our Country

THE COMMONS | OPINION

Everyone's Talking About 'Affordability.' Philanthropy Should, Too.

SOLUTIONS

MacKenzie Scott Gave Us $60 Million. We're Giving It Away.