Development donations pollute politics

MY TURN
by Lisa Markovitz

We often hear complaints about money in politics at every level impacting national, state and local campaigns.

While we all would like to see community interests prioritized over special interests, what are "special interests"? Don't all people have a special interest when it comes to their own opinions on the issues?

Of course, but when someone can donate money to a political official, who can make decisions that benefit the donor financially, then that is just wrong.

Ethics laws disallow taking money from those you can financially benefit. For instance, you cannot give a judge money who is about to decide your case. Land use should be no different.

It is time for Howard County community interests to outweigh special interests in order to level the playing field on quality of life decisions in land use.

Even if we trust our political officials to not be swayed by contributions, when a large part of their job involves one industry, shouldn't the appearance of a conflict just be removed?

A state bill was introduced last year to require recusal of county council members who receive contributions from those petitioning them for zoning changes, but it didn't get enough support from our state elected officials.

Now, we need to ask our Howard County state legislators to get behind a new bill, with bipartisan support, to prohibit developers/builders from donating to campaign accounts of the county executive and county council, since they regulate their financial interests so frequently. Elected officials should not even have the appearance of a conflict.

"Neighboring counties have laws banning developer contributions in county political races, and Howard County should do the same."

Neighboring counties have laws banning developer contributions in county political races, and Howard County should do the same.

Prince George's County has had a law of this type for decades. Montgomery County has one, and Baltimore County recently enacted one as well.

Even after the Supreme Court decision (Citizens United vs. Federal Election Commission) which gives broad rights for political donations, these local laws have stood up because of the financial conflict of interest in local regulatory work.

All the caps and limits that the Maryland Board of Elections enforces have legally stood as well.

Notably, many developer donations are often higher than they appear because the contributions often end up over the set limits by having "agents" contribute and using other loopholes.

I have heard from members of the building industry that they would support a ban on contributions because it would level the playing field for all developers. There would be no question about who donated and how much.

The People's Voice Howard County civic/political organization is sponsoring a petition asking our state legislators to get a law on the books for Howard County. You can find petition at www.ipetitions.com/petition/stop-developer-donations. Support and sign the petition to let our lawmakers know it is time to forbid these contributions.

It is time to make it harder for special interests to funnel funds to campaigns to gain influence over the interests of our general community, the environment and even the county's own fiscal health.

Lisa Markovitz is president of the Maryland civic/political group, The People's Voice.

YOUR TURN

Share your views on this month's My Turn. Submissions must be signed, include a phone number and email address. Please keep your comment to 250 words or less and send them to info@bizmonthly.com

Is data breach just waiting to happen?

BBB ADVICE
by Angie Barnett

When we hear about data breaches it seems like they are all big, hundreds of millions of records that were hacked.

According to CNBC, the biggest data breach of 2019 happened to Zynga, which produces mobile games including the wildly popular "Words With Friends." More than 218 million records were hacked in that breach.

Capital One announced a massive data breach in July 2019 and revealed more than 100 million accounts were breached.

The last thing you want to have your company's data breached, exposing your clients' information for all to see. If you're a small business owner and don't think a data breach can happen to you, think again.

The MidYear QuickView Data Breach Report found that more than 3,800 publicly disclosed data breaches were reported in the first six months of 2019. Those breaches exposed 4.1 billion compromised records. The report found 3.2 billion of those records were exposed in the eight biggest breaches.

"The majority of breaches reported this year had a moderate to low severity score," the report stated and exposed 10,000 or fewer records.

According to Forbes, the report shows "businesses of all sizes need to get their security act together … Many businesses wrongly assumed they are too small to be on the radar of the threat actors. The truth is that it is all about the data, and small businesses often have less well-guarded data stores."

"The majority of breaches reported this year had a moderate to low severity score."

What can you do to protect your business and your clients?

Sontiq, a high-tech security and identity protection company in Nottingham, Maryland, has several tips that help keep your business safe from hackers:

Create strong passwords.

Be original and use more than one word, swap out letters for numbers or other characters (such as 3 for E or ! for i) and vary capitalization.

Watch out for phishing scams.

Fake emails can look real, always be cautious when something doesn't seem right. If you're not sure of the validity – email the requester directly and confirm before sending files or clicking links.

Avoid over-sharing online.

Social media isn't private. Facebook, Twitter and LinkedIn have all had massive data breaches in recent years – be mindful of what to share and keep your privacy settings locked down.

Use IT best practices at home.

Although everyone hates getting a forced update, make sure to stay current with your operating system and security patches and be sure to have an active anti-virus software running in the background.

Store and transfer data cautiously.

Encrypt flash drives or files – think about what would happen if they were left on a plane or fell into the wrong hands.

Eliminate the paper trail.

Shred any papers with account information, social security numbers and other identifying information, along with credit card offers, bank courtesy checks and documents with your signature.

Monitor your accounts.

Keep a close eye on your accounts, look for suspicious activity and stay vigilant.

Angie Barnett is president and CEO of the Better Business Bureau of Greater Maryland.