PRIORITIZING PAYMENT PROCESSING SECURITY

We prioritize your security and strive to maintain a trustworthy environment for all customers.

Fraudulent Transactions are Increasing Industry-Wide

Volumes of bogus transactions (often called “carding attacks”) are on the rise throughout the nonprofit industry. These attacks are typically occurring in the evening or on weekends when most nonprofit staff are out of the office, thereby greatly reducing the chances that they could be quickly noticed and stopped.

At Humanitru, we take this matter seriously and want to ensure that you’re equipped with the necessary tools to protect your organization. To shield your account and finances, we highly recommend reviewing and adjusting your fraud settings with your payment processor to enhance your security measures, as well as reaching out to them directly so you can learn more about any additional safeguards you can put in place.

Why is This Important?

Payment processors may hold your organization responsible for chargeback fees if fraudulent transactions are not voided within 24 hours, and/or charge attempt fees for these fraudulent transactions. With attacks pushing dozens of transactions through per minute, it’s clear to see how this could become a very expensive problem if the proper preventative measures aren’t in place.

It’s imperitive that your organization takes all available measures to ensure that the security measures available from your payment processor are utilized to ensure that you aren’t gambling with either your finances or your supporters’ trust.

How Humanitru is Helping:

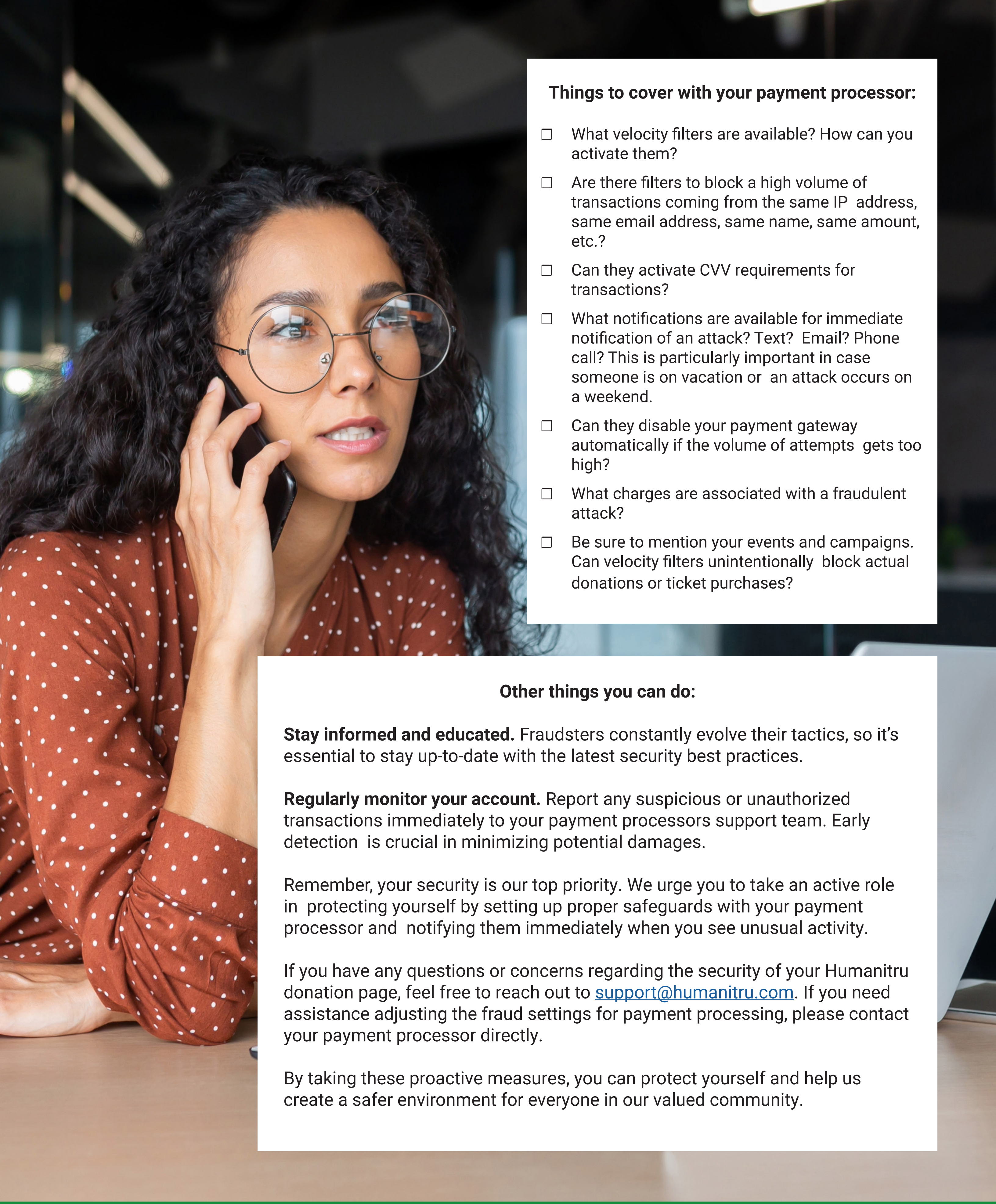
☑ Google reCAPTCHA is enabled on all Humanitru donation pages.

☑ Humanitru requires CVV entry on all credit card transactions.

☑ We monitor transaction volume and alert your organization to anomalies.

☑ For added security, Humanitru maintains our own security filters and monitoring. If one of our security filters is triggered by activity on your Pinecone landing page(s), we will email two main points of contact within your nonprofit (provided by you) to advise that your page is experiencing a suspicious issue. If the page continues to receive a high volume of suspicious activity and continues to fail our security filters, **we will temporarily suspend your Pinecone landing pages for your safety** and send another email notifying the same two contacts. This email will contain a button allowing you to reactivate your pages as you deem appropriate, or you can of course reach out to your Customer Success Manager or our Support Team for additional details and support.

To ensure you are swiftly notified in the event of an attack, please check that your contact details are accurate and updated regularly. If you'd like to know who are your current main points of contact, please contact your Humanitru support team at support@humanitru.com



Things to cover with your payment processor:

- ☐ What velocity filters are available? How can you activate them?
- ☐ Are there filters to block a high volume of transactions coming from the same IP address, same email address, same name, same amount, etc.?
- ☐ Can they activate CVV requirements for transactions?
- ☐ What notifications are available for immediate notification of an attack? Text? Email? Phone call? This is particularly important in case someone is on vacation or an attack occurs on a weekend.
- ☐ Can they disable your payment gateway automatically if the volume of attempts gets too high?
- ☐ What charges are associated with a fraudulent attack?
- ☐ Be sure to mention your events and campaigns. Can velocity filters unintentionally block actual donations or ticket purchases?

Other things you can do:

Stay informed and educated. Fraudsters constantly evolve their tactics, so it's essential to stay up-to-date with the latest security best practices.

Regularly monitor your account. Report any suspicious or unauthorized transactions immediately to your payment processors support team. Early detection is crucial in minimizing potential damages.

Remember, your security is our top priority. We urge you to take an active role in protecting yourself by setting up proper safeguards with your payment processor and notifying them immediately when you see unusual activity.

If you have any questions or concerns regarding the security of your Humanitru donation page, feel free to reach out to support@humanitru.com. If you need assistance adjusting the fraud settings for payment processing, please contact your payment processor directly.

By taking these proactive measures, you can protect yourself and help us create a safer environment for everyone in our valued community.