November 17, 2022

To my fellow Root Program and CA/B Forum Members,

For personal reasons, I was forced to step back from my daily routine as TrustCor's Chief Technology Officer at the close of 2019. The time between then and now has been unusual and challenging for us all. Just a few weeks ago, I was contacted by Joseph Menn (The Washington Post) regarding TrustCor. I could not connect with Joseph at that moment due to an unexpected and stressful move with my three children—and I would not learn what the inquiry was about until the end of last week.

I couldn't help but notice Mr. Menn wrote in his article that he did not hear back from any representative of TrustCor, even though he heard back from me, and from the company, both of which are documented in an attachment to this letter. Despite the company's timely responses and interest to be given a voice, it seems Mr. Menn and the Washington Post had other ideas and went ahead with an incomplete story. I was disappointed to read such a poor representation of the company, and what might have been avoided had he practiced a different style of journalism—different from rushing out what appears to simultaneously be an anti-privacy and anti-government story published on a US Election Day.

Normally in life, an injury or wrongdoing occurs before anyone is publicly threatened and shamed or even accused of doing something wrong. But in this case, our nearly 10-year-old company, which has operated without any mis-issuance and without any evidence or accusation of violation of conduct, policy or procedure was given that odd experience. With nearly a decades-long track record, and in one of the most audited and publicly-regulated micro-industries in the world, TrustCor is being called out to respond to a powerful non-profit and three gigantic public companies as though it has no track record at all. And, this has all occurred without a single conversation or inquiry with us, in trust.

We created TrustCor with the vision to provide state-of-the-art, simple-to-use, privacy enhancing products and services. To realize our goals, we knew we needed to be a CA, for which our customers—including the public—and the business we built would be beneficiaries. We have always been a small team, and I'm incredibly proud of our accomplishments. As we have been put into the spotlight, our jobs have become more difficult as so many eyes are on us to see if we succeed or fail. We have a deeper responsibility to our customers and to each other – and we'll continue to gain a larger audience to whom we owe a duty to "do the right thing, always." We each joined TrustCor, excited by the chance to build a new business focused on privacy – and to increase communications security for as many people as we could. We showed up every day through good and some not-so-good times because we felt a purpose, relished the challenge, and were inspired by the promise of improving privacy for

people globally. We have always understood with root certificate power comes great responsibility.

Some will remember a paper published at the 8th USENIX Security Symposium (August 1999), titled "Why Johnny Can't Encrypt." Most of the problems in the paper still existed when we started, and frankly, still exist today. Most regular people lack the expertise to use encryption technology, particularly with email properly. For these reasons and more, we created MsgSafe.io. MsgSafe.io is a separate business, with no special connections to the CA business or platform and treated like any other using the CA's customer-facing APIs. Unlike TrustCor's CA, MsgSafe.io is a globally distributed platform with web-based user experiences and interoperation with existing mainstream email clients. That product includes email, domain registration and DNS, and interoperability with other online products and services.

We understand our MsgSafe.io business is perceived as controversial by some — like other service offerings that focus on email privacy; we get targeted by more malware and ransomware perpetrators than other services. Unfortunately, this sometimes makes us look bad, even though MsgSafe.io actively mitigates these events. That said, Google's Gmail is probably still the worst offender of being a source of e-mail-based spam and malware on the planet.

While it has been repeatedly stated that there is no evidence of wrongdoing on the part of TrustCor, we have taken these accusations to heart and performed our own review to assess the merit of the claims. We appreciate the opportunity and transparency to respond to these claims regardless of their source and irrespective of how they make us feel. And, we are grateful for the mutual respect and support of our friends we've made over many years at CAB/F both face to face in meetings and on calls.

Along with some help from others, we have discovered that our accusers wear many different hats, interchangeably as it suits their narrative, ranging from university researchers to paid consultants and entrepreneurs, whose security products and services will likely benefit from the media exposure they create. These researchers lack in-depth operational, policy, and business expertise relative to CA operations. They are paid by public contracts with the US's Department of Defense, Federal Trade Commission, and Department of Homeland Security. Their claims are based on the mis-association of one company with another, and now through the transitive property are accusing everything with any touchpoint to be related, which is both irresponsible and error-prone. The journalists and a few web searches seem to connect the researchers back to other "collaborators" through a variety of relationships ranging from paid commercial deals, to personal friendships, and media tips to include two US Senators with strong views on privacy, a senate staffer who deals with privacy advocacy, the USA Federal Trade Commission, a Scandinavian reporter and other international researchers,

journalists and others. There are many interests at play with these gentlemen, including considerable self-interest.

We expected we would go through periods when we would be misunderstood. It's during these days, regardless of the ups and downs, that we try to focus on our work: on benefitting privacy, and executing with the highest of standards. Our world just got bigger.

I only ask you to please take the time to understand the situation fully, to read the actual information for yourselves instead of relying upon biased opinions presented by others, and most importantly to trust a decade-long positive track record, and remember the purpose of audited attestations and controls in the first place, before you make any decisions. I fear this sets an untenable precedent related to recursive shareholder-of-shareholder enumeration (which for some root program members may not even be possible) and casts doubt upon this well-established system of controls. I think doing so is discourteous to each other and counterproductive to those we all hope to serve.

As Rachel has said, we welcome our peers and root program administrators to additional non-public information or to add to our audited management attestations or whatever else might assuage your concerns and satisfy your interests evidencing the false claims and mischaracterizations levied against us.

Respectfully submitted,

Wylie Swanson, CTO

ATTACHMENT 1