Wednesday, March 11, 2009

Tony Webster
[redacted]
612-424-5426

Via United States Certified Mail, Return Receipt Requested to:

The Honorable Lori Swanson
Minnesota Attorney General
1400 Bremer Tower
445 Minnesota Street
St. Paul, MN 55101

RE: **Release and Publication of Personal and Financial Information by Norm Coleman**

Dear Ms. Attorney General:

I am writing to you to regarding the legal issues behind the publication of private and confidential donor information, including payment card information, by the campaign of former Senator Norm Coleman. I further write to you to seek the involvement of your office in the investigation and prosecution of the Coleman campaign for their violations of Minnesota Statutes, §325E.61 and §325E.64.

As an independent web developer and supporter of data privacy laws and legislation, this case especially concerns me as it develops in the national media spotlight without regard for the protection of the information of individual donors.

Background

On Wednesday, January 28, 2009, several regional and national political news sources and blogs investigated an apparent website failure at the Coleman campaign and independent contributors, including me, made the determination that the Coleman campaign forged the crash of their website to inflate the public perceptions of popularity of a new section on their website relating to recount efforts in the 2008 Minnesota Senate election.

The Coleman campaign, presumably during the process of changing the configuration options on their web server, erroneously changed the directory of their website to a higher level directory that contained website maintenance scripts, web server logs and a copy of a database file[1].

That database file was later identified by an anonymous contributor to the website WikiLeaks.org to contain a list of the names, addresses and other personal information of 51,641 supporters and website users of the Coleman campaign. Even worse, the database allegedly contained a list of web-based contributions to the Coleman campaign. That list contained names, addresses, credit card numbers, expiration dates and card security codes, employer and occupation information and the amount of the donation.

---

[1] Web consultant and blogger Adria Richards investigates the technical issues behind the publication of the database on the Internet, and posts images documenting how the Coleman campaign released their own database contents at http://butyoureagirl.com/2009/01/28/did-norm-coleman-fake-his-own-website-death/

Those files have been exported from a database file to Microsoft Excel spreadsheets published on the WikiLeaks website on Tuesday, March 10, 2009[2], and WikiLeaks sent e-mails to individual donors advising them that their personal and payment information had been compromised and shared with WikiLeaks, in case the Coleman campaign hadn't properly notified them of their publication and release of donor information. In an e-mail from WikiLeaks:

> "Your name, address and other details appear on a membership list leaked to us from the Norm Coleman Senate campaign. We understand that Norm Coleman became aware of the leak in January."

In an e-mail sent today from Coleman Campaign Manager Cullen Sheehan to donors, Sheehan acknowledged the e-mail from WikiLeaks to donors and the campaign, and blamed the situation on a firewall breach. This e-mail took no responsibility for the storage nor publication of the database file, and stated that federal authorities "…did not find any evidence that [their] database was downloaded by any unauthorized party."

The Coleman Campaign's claim of a "Firewall Breach"

In the e-mail sent today from Coleman Campaign Manager Cullen Sheehan to donors, Sheehan stated that in January, "…an event occurred that made us fearful that our firewalls might have been breached."

Sheehan's claim of not only the existence of a firewall, but also a breach of it, is a complete fabrication. Firewalls, however portrayed in the media and in society, have very limited capabilities. A firewall could block incoming connections to specific addresses and ports, but in this case, the actual database was not breached. The Coleman campaign took the active step of exporting the contents of their database into a file. They then placed that file in a publicly accessible area of their web server and published that file for anyone on the Internet to download.

If a firewall existed, and because of the active role the Coleman campaign took in exporting the database contents[3], the firewall would not be able to distinguish the difference between the downloading of the database file and the downloading of any other website content – including images, videos or text.

Furthermore, it would have taken no special tools or knowledge to download the file from the Coleman campaign website. Any Internet user with a web browser could have followed links appearing on the Coleman campaign website to download the database file.

Sheehan's attempt to blame individuals external to the publication and release of the credit card data is an attempt to deflect legal action and/or investigation against the campaign.

Storage of Credit Card Numbers, Expiration Dates and Card Security Codes

---

[2] Two Microsoft Excel spreadsheets are available for download at http://wikileaks.org/wiki/The_Big_Bad_Database_of_Senator_Norm_Coleman

[3] There was no "breach" because the database was exported to a file that was placed in a publicly accessible area of the website. Based on the best information available, the MySQL database itself was not accessed by an unauthorized party. The Coleman campaign, likely in the process of the administration of the web server, exported the database contents and improperly stored them on the web server.

It's clear that the Coleman campaign took the active role in the exporting of the contents of the database, the publication of the database file to the internet, but even more interesting is the actual contents of the database.

As a website that accepts payments via credit card, the Coleman campaign is bound by the Payment Card Industry Data Security Standards (PCI DSS)[4], a unified set of rules agreed to by all major credit card companies, banks and card processing services. According to the PCI DSS, Requirement 3, the storage of credit card numbers is permitted as long as it is "…required for business, legal and/or regulatory purposes." In any case, the card number *must* be protected by encryption. If the expiration date is stored, it must also be encrypted. In no case should the three or four-digit security code on the back of a credit card *ever* be stored, regardless of the reason and regardless of the protection or encryption used.

It's questionable that the Coleman campaign had any requirement to store any more than the last four numbers of a credit card number for accounting purposes, but the database file actually contained the full credit card number, expiration date and card security code of the cardholder.

At this point, it's clear that the Coleman campaign took several negligent steps in the matter: (a) the improper storage and collection of full credit card numbers, expiration dates and card security codes, (b) the database contents being exported from the database to a database file, (c) the misconfiguration of the Coleman campaign website, and (d) the further publication of the database file to the internet.

Legal Violations by the Coleman Campaign

The Coleman campaign admits in their e-mail to donors that they were aware that they had published the database file, mistakenly or otherwise, back in January. However, several news articles from January go into detail about the publication of the database by the Coleman campaign.

The Coleman campaign has violated Minnesota Statutes, §325E.61, which requires the campaign to take specific actions in the event of the release of an individual's first and last name in combination with an "account number to a credit or debit card number, in combination with a security code…" Pursuant to the same, the campaign must provide notice to the cardholders and coordinate with consumer reporting agencies.

Notifying the public and the media over a month after the campaign's publication of the database file is a violation of the trust of the campaign's donors, and was likely done in the interests of the political nature of this event.

The Coleman campaign has further violated Minnesota Statutes, §325E.61 for the storage of card security codes after 48 hours.

Legal Action Against the Coleman Campaign

I'm writing to you to request that your office collaborates with investigative and law enforcement authorities to charge and fine the Coleman campaign for the publication and distribution of personal financial information, the illegal storage of card security codes after 48 hours of the approval of a transaction, neglecting to notify donors of the release of their personal and financial information. I would further request that your office seek a court order requiring the Coleman campaign to notify each

---

[4] The PCI DSS standards are described at http://en.wikipedia.org/wiki/PCI_DSS and can be viewed online at https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

individual donor via postal mail, notify card issuers or banks of the data theft and notify the media of their efforts to protect cardholder information.

Again, the specific violations of Minnesota Statute includes, but is not limited to:

1. **Minnesota Statutes, §325E.64(2)(3),** for "…[retaining] the card security code data… 48 hours after the authorization of the transaction." As a result of violating this statute, the Coleman campaign is liable for any cost associated with the cancellation or reissuance of cards, the closure of any affected accounts and the notification of cardholders.

2. **Minnesota Statutes, §325E.61(1),** for failing to notify cardholders regarding the "breach" or release of personal information in combination with the credit card number and card security code.

This is a very delicate and sensitive matter that requires immediate investigation and action. The Coleman campaign has shown itself to be untrustworthy in the handling of this matter, so I look to your office to assist in the prosecution and resolution of this matter to protect the financial information belonging to the individual donors.

If you have any questions regarding the details I've stated in this letter, or any assistance in the investigation of the Coleman campaign, please don't hesitate to contact me via phone at 612-424-5426.

Thank you for your time and assistance.

With warm regards,

[redacted]

Tony Webster

CC: Visa Fraud Investigations
Cardholder Information Security Program

MasterCard Site Data Protection
PCI Compliance

American Express
Data Security and PCI Compliance

Discover Network
Incident Response Team

United States Secret Service
Electronic/Financial Crimes Task Force
Minneapolis Field Office

Local Media Agencies