

Gerald Roylance  
1168 Blackfield Way  
Mountain View, CA 94040-2305  
December 8, 2014

**Before the  
Federal Communications Commission  
Washington DC 20544**

<b>In the matter of</b>	<b>CG Docket No. 02-278</b>
<b>United Healthcare Service's Petition for Expedited Declaratory Ruling</b>	<b>Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991</b>
	<b>DA 14-1614 November 6, 2014</b>

**Gerald Roylance's Comments re American Bankers Association Petition**

In DA 14-1614,<sup>1</sup> the FCC seeks comment about the American Bankers Association's petition.<sup>2</sup> Generally, the petition wants a 227(b) exemption for free-to-end-user messages for 4 categories. I oppose any exemption.

When Congress passed the TCPA, it made a finding that consumers do not like automated messages no matter what the content. I believe that should be the starting point of any automated message discussion. If a consumer wants automated messages from his bank, then he can give the bank prior express written consent for those messages. The TCPA has an appropriate mechanism for accomplishing tasks 1 through 3

---

<sup>1</sup> FCC, 6 November 2014, *Consumer and Governmental Affairs Bureau Seeks Comment on Petition for Exemption filed by the American Bankers Association.*, [https://apps.fcc.gov/edocs\\_public/attachmatch/DA-14-1614A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1614A1.pdf)

(fraudulent transactions, security breaches, and remedial action). For task 4 (money transfers), the recipient's bank should acquire prior express written consent.

If the ABA is correct in its view that all consumers want these messages, then its member banks should have no trouble acquiring PEWC. Then we are done. Why doesn't the ABA seek the direct solution?

Of course, ABA and others will then complain that cellular phone numbers may be reassigned. See footnote 30. That is the subject of other petitions before the lethargic FCC. ABA members can purchase access to databases that track reassignments. If we believe the Petition, then lots of money is at stake, so the access should not be a significant burden. There are other potential methods, too, such as periodic calls that will act appropriately when Special Information Tones are received.

The Petition presupposes that ABA members know the calls are going to cellular telephones. Sending a fraud alert text to a landline would be pointless.

Task 1 is worried about fraudulent transactions. I am torn here. My bank has called about fraudulent transactions on my credit card. It was a live call, and there was a lot of discussion back and forth. I live in California. Somebody in Missouri bought a \$500 iPhone from Wal-Mart using my credit card number. The iPhone was picked up at a Wal-Mart in Detroit. The transaction stinks to high heaven, but both Wal-Mart and the credit card company let it go through. After the first iPhone was picked up, the thief charged a second iPhone to my account. That's when the credit card company decided something was amiss, so it blocked the second transaction. Then I got a nice call from my bank asking if I'd made the first charge. Of course not. They removed the charge from my account.

My bank was not out any money on the deal: it hit Wal-Mart with a charge back. Wal-Mart, despite the dubious characteristics of the transaction, claimed that I must have

---

<sup>2</sup> American Bankers Association, 14 October 2014, *Petition for Exemption of the American Bankers Association*, <http://apps.fcc.gov/ecfs/document/view?id=60000973094>

made the charge. Why? Wal-Mart claimed it verified the transaction. That verification may have been as trivial such as the thief knowing my Zip code.

The fundamental problem here is that ABA members have crappy financial controls. My newspaper tells me that Europe and Asia have better systems, but American bankers do not want to adopt those systems. Instead they muddle through.

Any why shouldn't the banks muddle through? The merchants (not the banks) pay for the fraud. The merchants make allowances for the equivalent of high-tech shoplifting or shrinkage. (The banks lose money on credit card defaults, but those losses are covered by exorbitant interest rates.) The ABA members have a system that makes them a lot of money right now. Stupidly, they don't want to change it.

A waitress or a store clerk can swipe credit card information by swiping the card twice: once for the store and a second time for themselves. Once the credit card number, the verification code, and a few other facts are known, the clerk can charge other things. And what sophisticated step do ABA members take then? After the fraud has surfaced, they disable the account and change my credit card number. There's little security there. It's a system built on trust, and the crooks exploit that trust.

My take is that Task 1 is a band aid whose purpose is to make the merchant's a little happier. But how is it really supposed to work? The bank gets a request to charge a certain account, and the bank thinks the charge may not be appropriate. So it sends a text to me to confirm the charge? Is there going to be a long wait to see if I reply. Isn't it simpler just to decline the charge and not bother me? Or tell the merchant that more information is required?

There are better methods. I expect that credit card companies will get a lot of competition from ApplePay. Think about it. Consumers don't just have cellular telephones now, they have smartphones. Those phones can securely interact with point of sale terminals. Public key cryptosystems developed in the 1980s can prevent criminals from making fraudulent charges. The transactions can be done over wireless rather than

cellular connections. Modern systems can offer protection for the consumer, the bank, and the merchant.

Compare that to the backward automated system that ABA proposes. ABA wants to process transactions and earn fees. Instead of making the transaction fundamentally secure, the members employ ad hoc methods of looking for fraudulent transactions. When they find an unusual transaction, they want to send a text message? Why not start with the smartphone making a secure transaction.

Even bank check processing is backward. Yes, it is convenient to make a deposit by using a smartphone to image the check and send it to the bank. But think about that a little bit more. If smartphones are involved, then why are we using images instead of cryptosystems? It's a fax-machine mentality in a computer world.

(The medical world is also strange. My doctor can fax a prescription to my pharmacy – unless the prescription is for a narcotic. Then I have to get the prescription on a spiffy DEA form and take it to the pharmacy. The pharmacy then has to report the script to the DEA so statistics can be compiled. A cryptosystem is a beautiful solution here. It can verify the doctor, the patient, the pharmacy and the drug. It can be sent over the network but not reused.)

Task 2 is another band aid. Yes, there have been horrendous security breaches, but the fix is to strengthen the underlying security rather than make informing consumers inexpensive. In some ways, Task 2 doesn't even seem right. If Target has a security breach, then Target (not the bank) is supposed to inform me of that breach. Target may inform the banks that the credit card has been compromised, and then maybe the bank could tell me, but that also strikes me as backward.

A significant feature of Gramm-Leach-Bliley is the cost of notification. If a company messes up and its database is penetrated, then it needs to inform each of its customers. Postage and mailing is not cheap. If a company has 1 million customers, then it could be looking at \$1 million in notification costs. That is an incentive to make the database secure. I think Congress understood that cost and its incentive value. Making

notification cheap removes the incentive and ultimately reduces security. It does the wrong thing.

I'm sorry, but some friends have burned University of Chicago economics into my feeble head.

Task 3 is much the same as task 2. The ABA points to the “volume and frequency of these remediation notices”. ABA wants a cheap method of distribution, but that is not necessarily a good thing. When a company's records are breached and it pays for a year's worth of credit monitoring for its compromised customers, the savings offered by automated calls is small potatoes. It is such a little picture viewpoint.

I also have to wonder if task 3 is really practical. It will take more than 160 characters to explain some remediation, so is the intent to send 10 or 20 texts? See items 4 and 5 at Petition page 18 – sending as many texts as are needed. Sending an automated voice message is probably even less valuable. Who is going to remember the details of an unexpected voiceblast? It's a method that could meet the letter of GLB without the effectiveness. A letter (or even an email) is a far better method for describing remediation steps and procedures. People will want to review the information; it may take some time to understand the whole impact. I suspect the actual practice that the ABA intends is voice broadcasting or texting a URL to the consumer. That would drive communication costs to almost zero. That is not the intent of GLB.

Task 4 (money transfers) seems to be a narrow application, so I wonder why it is even mentioned. I think it is window dressing. Yes, the FCC gave an exemption to package delivery services, but I get lots of packages delivered to my door. Lots of people buy stuff from Amazon and other online or catalog outfits. Money transfers are something that eBay has told me to avoid. It's like sending cash, and once sent, it is gone. I've seen plenty of auctions on eBay that smell of fraud; they don't use PayPal, they want a wire transfer.

A couple days ago a Deputy Sheriff I know talked about wiring his son some money. It was a dicey proposition, and he didn't want to do it. The son was going

through a divorce, and his wife had emptied their joint account; the son needed some money. The game would be wiring the money to the account, but then the son would have to take it out before the wife found out that more cash was in the account. Instant notifications are not always good.

I don't see the necessity for exempting task 4. Maybe the ABA should develop an App for That. The payer and the payee can connect to each other, exchange any pertinent information, and execute the transaction. The bank need not contact the payee directly. Isn't that how point-of-sale terminals are supposed to work?

An exemption for these tasks is not necessary. Let consumers continue to have control over access to their cellular telephones and privacy rights. Do not give banks or others the absolute right to send automated messages. Banks have the means to obtain PEWC for these messages, and letting institutions use inexpensive notification methods will frustrate Congressional goals.

No matter what, any consumer should be permitted to opt out of automated messages or texts. Automated calls may be cheap and effective, but that does not mean that everybody welcomes them.

The Commission should take some time and consider how backward the ABA's Petition is. All a crook needs to do these days is hack into a system and grab some personal information. Then he can sell that information to some lower level crooks who will go on spending sprees until some fraud alert trigger is reached and the credit card is turned off. The crooks get to learn what triggers a turn off; they then evolve their sprees to keep the card going longer. The merchants raise prices to cover the chargebacks, and consumers pay more for the merchandise. The banks sit in the middle and make money. As far as fraud goes, to keep up appearances, they have some ad hoc systems that try to recognize fraudulent charges. Instead of making things secure, they want to make failure cheaper. That's not the way to go.

I'm not fond of PayPal, and there were some glitches in ApplePay, but improved financial transaction systems are developing. Asia has had pay-with-your-cellphone

vending machines for years. That's not a model that ABA members want. They kicked up a storm when the government wanted to cap transactions fees. Credit card companies require merchants to take all transactions, but that benefits the credit card company more than the merchant. The person ahead of me bought a \$1 candy bar with a credit card. I was shocked. Candy is probably a high profit item, but the transaction fee is a killer.

It's time for the ABA to evolve. Use intelligent cards and strong protocols. The FCC should not help the ABA dinosaur circumvent the evolutionary pressure of GLB.