

*Before the*  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554

In the Matter of:  
Protecting the Privacy of Customers of Broadband  
and Other Telecommunications Services

WC Docket No. 16-106

Louis Spadafora  
Payfone Inc.  
245 5<sup>th</sup> Ave  
Suite 1103  
NY, NY 10016

July 6, 2016

## Summary

### *The use of CPNI information for authentication and fraud detection for non-BIAS services*

Fraud occurring on a telecommunications or BIAS network is enabled by fraudsters impersonating the telecom customer or taking over the customer's telecommunications or broadband account. There are many ways impersonation and account take overs can occur: social engineering along with calls to customer service, SIM swaps and device changes under the guise that the device was lost, stolen or broken, etc. Our request is that the provisions for allowing CPNI data to be used for the purposes of authenticating and preventing fraud be modified to explicitly state that non-BIAS services, such as financial transactions and commerce transactions, fall within the allowed uses of CPNI data without the need to collect explicit customer consent.

## Comments

### *Paragraph 115.*

There are 2 concerns with the wording of paragraph 115:

1. Telecommunications and BIAS providers are not comfortable using data without consent for authentication and fraud prevention for non-BIAS services, such as financial services.
2. The BIAS and telecommunications providers currently treat authentication and fraud prevention for non-BIAS products similar to marketing use cases and are requiring explicit opt-in and opt-out customer consent. A requirement that a customer must provide opt-in consent for fraud prevention fails to protect consumers, as fraudsters will not opt-in to be authenticated prior to a transaction, and in the event of an account take over, the fraudster can simply opt-out.

Telecommunications and BIAS providers interpret the non-consent uses of CPNI as allowing the BIAS providers to protect only BIAS assets, and the customer from fraudulent uses of the services provided by the BIAS provider. Under today's rules, BIAS providers are not comfortable using CPNI to protect customers from fraudulent use of non-BIAS products and services on the BIAS network, such as financial transactions. In fact, some BIAS providers believe it's the intent of the FCC to require the BIAS provider to allow customers to opt-out of using CPNI information for authentication and fraud prevention, even if the customer has given consent to the financial institution (FI) via the FI's terms and conditions, which state what information will be used by their carrier.

The intent is to use CPNI information to authenticate the consumer and prevent fraudulent transactions on the BIAS network, resulting from SIM swaps, account take overs and other forms of fraud. However, the 4 major carriers, AT&T, Sprint, T-Mobile and Verizon, all believe consent to the non-BIAS service provider, such as an FI, is required to provide information to authenticate consumers and prevent fraudulent transactions for non-BIAS services. Some even require explicit consent, and believe the FCC will require the ability for a consumer to opt-out of the use of their data that could be used to authenticate a financial transaction, which leaves significant security flaws since fraudsters don't give consent to be authenticated.

To clarify, we are asking that CPNI data be "used" to create fraud indicators that can be shared with non-BIAS providers to prevent impersonation and fraud to consumers. For example, account information, SIM data, or IMEI information can be used to generate a risk, or fraud, indicator derived from the fact account or device data has changed is sufficient.

*Paragraph 116.*

Non-consent uses of location information do not include the ability to use such location information for the purposes of preventing consumer fraud. With respect to location information, fraud use cases require the same level of consent as marketing use cases. However, fraudsters will not agree at the time of a transaction to allow location information to be used to authenticate them.

If a financial transaction is occurring in NYC and the BIAS provider believes the account holder is in Miami, the financial institution may require additional levels of authentication prior to allowing the transaction if the location discrepancy was made available.

To protect against fraud, and at the same time ensure the customer's privacy is maintained, location used for fraud purposes can be Course Location. Course Location can be defined as cell location, or location with a 10 KM radius (or some broader radius). To further protect the customer's privacy, a telecommunications or BIAS provider could provide a response indicating if a customer is within the course location, rather than sharing actual location information. Meaning, the BIAS could simply say yes or no if the customer's location is within the course distance of a location passed to the BIAS. The intent is to simply validate if a customer is actually near the location where a transaction is being made.

*Paragraph 117, footnote 199.*

47 U.S.C. § 222(d)(2)

“to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services”).

Telecommunications and BIAS providers are conservatively interpreting this language to mean that CPNI data cannot be used without consent for the purposes of authentication and fraud prevention when the service is not a BIAS service that the data will be used to protect. For example, BIAS providers do not believe this provision gives them the ability to use CPNI data for the purposes of ensuring that a financial transaction is not fraudulent. Events such as a recent SIM swap or device change immediately prior to a financial transaction could be an indication the telecom account has been taken over and the transaction is being initiated by a fraudster. The BIAS providers believe use data to authenticate a transaction is similar to marketing use cases and falls under Part III.C.1.c “Customer Approval Required for Use and Disclosure of Customer PI for All Other Purposes” (paragraph 127).

*Paragraph 118.*

This provision allows data to be shared “...when doing so will help protect customers from abusive, fraudulent or unlawful robocalls.” Can we propose that the wording be modified to state “...from abuse, fraud or unlawful robocalls.” The intent for requesting this change is the ability to also protect the customer from impersonation. Today, fraudsters can utilize legal applications to impersonate a customer by spoofing their phone number. The fraudster will call a financial institution pretending to be the customer and gain access to their financial account and personal information, by spoofing the customer's caller ID using a legally obtain application. In addition, fraudulent incoming calls, calls made to the customer for the purposes of social engineering and phishing, are not necessarily robocalls. A modification to the proposed wording will allow services to protect the customer from fraudulent, non-robo attacks for both incoming calls to the customer as well as calls impersonating the customer.