Complaint Feedback Loop Address Header

Abstract

This document describes a method that allows a Message Originator to
specify a Complaint Feedback Loop (CFBL) address as a message header
field. It also defines the rules for processing and forwarding such
a complaint. The motivation for this arises out of the absence of a
standardized and automated way to provide Mailbox Providers with an
address for a CFBL. Currently, providing and maintaining such an
address is a manual and time-consuming process for Message
Originators and Mailbox Providers.

The mechanism specified in this document is being published as an
experiment to gather feedback and gauge the interest of implementers
and deployers. This document is produced through the Independent RFC
Stream and was not subject to the IETF's approval process.

Status of This Memo

This document is not an Internet Standards Track specification; it is
published for examination, experimental implementation, and
evaluation.

This document defines an Experimental Protocol for the Internet
community. This is a contribution to the RFC Series, independently
of any other RFC stream. The RFC Editor has chosen to publish this
document at its discretion and makes no statement about its value for
implementation or deployment. Documents approved for publication by
the RFC Editor are not candidates for any level of Internet Standard;
see Section 2 of RFC 7841.

Information about the current status of this document, any errata,
and how to provide feedback on it may be obtained at
https://www.rfc-editor.org/info/rfc9477.

Copyright Notice

Table of Contents

1. Introduction and Motivation

   This memo extends the CFBL recommendations described in [RFC6449]
   with an automated way to provide the necessary information by the
   Message Originator to Mailbox Providers. The reader should be
   familiar with the terminology and concepts in that document. Terms
   beginning with capital letters used in this memo are described in
   that document.

   As described in [RFC6449], the registration for such a CFBL needs to
   be done manually by a human at any Mailbox Provider that provides a
   CFBL. The key underpinning of [RFC6449] is that access to the CFBL
   is a privilege and Mailbox Providers are not prepared to send
   feedback to anyone they cannot reasonably believe are legitimate.
   However, manual registration and management can be quite time-
   consuming if there are new feedback loops rising up or if the Message

Originator wants to add new IP addresses, DomainKeys Identified Mail (DKIM) domains, or change their complaint address. In addition, a manual process is not well suited or feasible for smaller Mailbox Providers.

Here, we propose that Message Originators add a header field without the need to manually register with each Feedback Provider and willing Mailbox Providers can use it to send the Feedback Messages to the specified complaint address. This simplification or extension of a manual registration and verification process would be another advantage for the Mailbox Providers.

A new message header field, rather than a new DNS record, was chosen to easily distinguish between multiple Message Originators without requiring user or administrator intervention. For example, if a company uses multiple systems, each system can set this header field on its own without requiring users or administrators to make any changes to their DNS. No additional DNS lookup is required of the Mailbox Provider side to obtain the complaint address.

The proposed mechanism is capable of being operated in compliance with data privacy laws, e.g., the EU's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). As described in Section 6.4, a Feedback Message may contain personal data. This document describes a way to omit this personal data when sending the Feedback Message and only send back a header field.

Nevertheless, the described mechanism below potentially permits a kind of person-in-the-middle attack between the domain owner and the recipient. A bad actor can generate forged reports to be "from" a domain name the bad actor is attacking and send these reports to the CFBL address. These fake messages can result in a number of actions, such as blocking accounts or deactivating recipient addresses. This potential harm and others are described with potential countermeasures in Section 6.

In summary, this document has the following objectives:

* Allow Message Originators to signal that a complaint address exists without requiring manual registration with all providers.

* Allow Mailbox Providers to obtain a complaint address without developing their own manual registration process.

* Have the ability to provide a complaint address to smaller Mailbox Providers who do not have a feedback loop in place

* Provide a data privacy safe option for a CFBL.

1.1. Scope of this Experiment

The CFBL-Address header field and the CFBL-Feedback-ID header field comprise an experiment. Participation in this experiment consists of adding the CFBL-Address header field on the Message Originator side or by using the CFBL-Address header field to send Feedback Messages to the provided address on the Mailbox Provider side. Feedback on

the results of this experiment can be emailed to the author, raised as an issue at <https://github.com/jpbede/rfc-cfbl-address-header/>, or can be emailed to the IETF cfbl mailing list (cfbl@ietf.org).

The goal of this experiment is to answer the following questions based on real-world deployments:

*   Is there interest among Message Originators and Mailbox Providers?

*   If the Mailbox Provider adds this capability, will it be used by the Message Originators?

*   If the Message Originator adds this capability, will it be used by the Mailbox Providers?

*   Does the presence of the CFBL-Address and CFBL-Feedback-ID header fields introduce additional security issues?

*   What additional security measures/checks need to be performed at the Mailbox Provider before a Feedback Message is sent?

*   What additional security measures/checks need to be performed at the Message Originator after a Feedback Message is received?

This experiment will be considered successful if the CFBL-Address header field is used by a leading Mailbox Provider and by at least two Message Originators within the next two years. It will also be considered a success if these parties successfully use the address specified in the header field to exchange Feedback Messages.

If this experiment is successful and these header fields prove to be valuable and popular, the header fields may be taken to the IETF for further discussion and revision.

1.2. How CFBL Differs from One-Click-Unsubscribe

For good reasons, the One-Click-Unsubscribe [RFC8058] signaling already exists and may have several interests in common with this document. However, this header field requires the List-Unsubscribe header field. The purpose of this header field is to provide the link to unsubscribe from a list. For this reason, this header field is only used by operators of broadcast marketing lists or mailing lists and not in normal email traffic.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

In this document, "CFBL" is the abbreviation for "Complaint Feedback Loop" and will hereafter be used.

Syntax descriptions use ABNF [RFC5234] [RFC7405].

3. Requirements

3.1. Received Message

This section describes the requirements that must be met for the
following: a received message, the message that is sent from the
Message Originator to the Mailbox Provider, and a report that is to
be sent later.

3.1.1. Strict

If the domain in the RFC5322.From and the domain in the CFBL-Address
header fields are identical, this domain MUST be matched by a valid
[DKIM] signature. In this case, the DKIM "d=" parameter and the
RFC5322.From field have identical domains. This signature MUST meet
the requirements described in Section 3.1.4.

The following example meets this case:

```
Return-Path: <sender@mailer.example.com>
From: Awesome Newsletter <newsletter@example.com>
To: receiver@example.org
Subject: Super awesome deals for you
CFBL-Address: fbl@example.com; report=arf
Message-ID: <a37e51bf-3050-2aab-1234-543a0828d14a@mailer.example.com>
Content-Type: text/plain; charset=utf-8
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=news;
      h=Subject:From:To:Message-ID:CFBL-Feedback-ID:CFBL-Address;
```

This is a super awesome newsletter.

3.1.2. Relaxed

If the domain in CFBL-Address header field is a child domain of
RFC5322.From, the RFC5322.From domain MUST be matched by a valid
[DKIM] signature. In this case, the DKIM "d=" parameter and the
RFC5322.From domain have an identical (Example 1) or parent (Example
2) domain. This signature MUST meet the requirements described in
Section 3.1.4.

Example 1:

```
Return-Path: <sender@mailer.example.com>
From: Awesome Newsletter <newsletter@mailer.example.com>
To: receiver@example.org
Subject: Super awesome deals for you
CFBL-Address: fbl@mailer.example.com; report=arf
Message-ID: <a37e51bf-3050-2aab-1234-543a0828d14a@mailer.example.com>
Content-Type: text/plain; charset=utf-8
DKIM-Signature: v=1; a=rsa-sha256; d=example.com;
      h=Content-Type:Subject:From:To:Message-ID:
      CFBL-Feedback-ID:CFBL-Address;
```

This is a super awesome newsletter.

Example 2:

```
Return-Path: <sender@mailer.example.com>
From: Awesome Newsletter <newsletter@example.com>
To: receiver@example.org
Subject: Super awesome deals for you
CFBL-Address: fbl@mailer.example.com; report=arf
Message-ID: <a37e51bf-3050-2aab-1234-543a0828d14a@mailer.example.com>
Content-Type: text/plain; charset=utf-8
DKIM-Signature: v=1; a=rsa-sha256; d=example.com;
      h=Content-Type:Subject:From:To:Message-ID:
      CFBL-Feedback-ID:CFBL-Address;

This is a super awesome newsletter.
```

3.1.3. Third Party Address

If the domain in RFC5322.From differs from the domain in the CFBL-Address header field, an additional valid [DKIM] signature MUST be added that matches the domain in the CFBL-Address header field. The other existing valid [DKIM] signature MUST match the domain in the RFC5322.From header field. This double DKIM signature ensures that both the domain owner of the RFC5322.From domain and the domain owner of the CFBL-Address domain agree on who should receive the Feedback Messages. Both signatures MUST meet the requirements described in Section 3.1.4.

The following example meets this case:

```
Return-Path: <sender@saas-mailer.example>
From: Awesome Newsletter <newsletter@example.com>
To: receiver@example.org
Subject: Super awesome deals for you
CFBL-Address: fbl@saas-mailer.example; report=arf
Message-ID: <a37e51bf-3050-2aab-1234-543a0828d14a@example.com>
Content-Type: text/plain; charset=utf-8
DKIM-Signature: v=1; a=rsa-sha256; d=saas-mailer.example; s=system;
      h=Subject:From:To:Message-ID:CFBL-Feedback-ID:CFBL-Address;
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=news;
      h=Subject:From:To:Message-ID:CFBL-Feedback-ID:CFBL-Address;

This is a super awesome newsletter.
```

An Email Service Provider may accept pre-signed messages from its Message Authors, making it impossible for it to apply the double signature described above; in this case, the double signature MUST be omitted and the Email Service Provider MUST sign with its domain. Therefore, the pre-signed message MUST NOT include "CFBL-Address" and "CFBL-Feedback-ID" in its "h=" tag.

This way, the Email Service Provider has the possibility to accept the pre-signed messages and can inject their own CFBL-Address.

The following example meets this case:

```
Return-Path: <newsletter@example.com>
```

```
From: Awesome Newsletter <newsletter@example.com>
To: receiver@example.org
Subject: Super awesome deals for you
CFBL-Address: fbl@saas-mailer.example; report=arf
Message-ID: <a37e51bf-3050-2aab-1234-543a0828d14a@example.com>
Content-Type: text/plain; charset=utf-8
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=news;
        h=Subject:From:To:Message-ID;
DKIM-Signature: v=1; a=rsa-sha256; d=saas-mailer.example; s=system;
        h=Subject:From:To:Message-ID:CFBL-Feedback-ID:CFBL-Address;

This is a super awesome newsletter.
```

3.1.4. DKIM Signature

When present, CFBL-Address and CFBL-Feedback-ID header fields MUST be included in the "h=" tag of the aforementioned valid DKIM signature.

If the domain is not matched by a valid DKIM signature or the header field is not covered by the "h=" tag, the Mailbox Provider SHALL NOT send a report message.

3.2. Multiple CFBL-Address Header Fields

A Message can contain multiple CFBL-Address header fields. These multiple header fields MUST be treated as a list of addresses, each of which should receive a report.

3.3. CFBL-Feedback-ID Header Field

The Message Originator MAY include a CFBL-Feedback-ID header field in its messages for various reasons, e.g., their feedback loop processing system can't do anything with the Message-ID header field.

It is RECOMMENDED that the header field include a hard-to-forge protection component, such as an [HMAC] using a secret key, instead of a plaintext string.

3.4. Receiving Report Address

The receiving report address provided in the CFBL-Address header field MUST accept [ARF] reports.

It is OPTIONAL for the Message Originator to request a [XARF] report, as described in Section 3.5.1.

3.5. Feedback Message

The Feedback Message (sent by Mailbox Provider to the address provided in the CFBL-Address header field) MUST have a valid [DKIM] signature. This signature MUST match the RFC5322.From domain of the Feedback Message.

If the message does not have the required valid [DKIM] signature, the Message Originator SHALL NOT process this Feedback Message.

The Feedback Message MUST be an [ARF] or [XARF] report. If the Message Originator requests it (described in Section 3.5.1) and it is technically possible for the Mailbox Provider to do so, the Feedback Message MUST be a [XARF] report. Otherwise, the Feedback Message MUST be an [ARF] report.

The third MIME part of the [ARF] or the "Samples" section of the [XARF] report MUST contain the Message-ID [RFC5322] of the received message. If present, the CFBL-Feedback-ID header field of the received message MUST be added to the third MIME part of the [ARF] or to the "Samples" section of the [XARF] report.

The Mailbox Provider MAY omit or redact all further header fields and/or body to comply with any data regulation laws as described in [RFC6590].

3.5.1. XARF Report

A Message Originator wishing to receive a [XARF] report MUST append "report=xarf" to the CFBL-Address header field (Section 5.1). The report parameter is separated from the report address by a ";".

The resulting header field would appear as shown below.

CFBL-Address: fbl@example.com; report=xarf

4. Implementation

4.1. Message Originator

A Message Originator who wishes to use this new mechanism to receive Feedback Messages MUST include a CFBL-Address header field in their messages.

It is RECOMMENDED that these Feedback Messages be processed automatically. Each Message Originator must decide for themselves what action to take after receiving a Feedback Message.

The Message Originator MUST take action to address the described requirements in Section 3.

4.2. Mailbox Provider

A Mailbox Provider who wants to collect user actions that indicate the message was not wanted and to send a Feedback Message to the Message Originator MAY query the CFBL-Address header field and forward the report to the provided CFBL address.

The Mailbox Provider MUST validate the DKIM requirements of the received message described in Section 3.1 and MUST take action to address the requirements described in Section 3.5 when sending Feedback Messages.

5. Header Field Syntax

5.1. CFBL-Address

The following ABNF imports the rules for fields, CFWS, CRLF, and
addr-spec from [RFC5322]. Implementations of the CFBL-Address header
field MUST comply with [RFC6532].

```
fields =/ cfbl-address

cfbl-address = "CFBL-Address:" CFWS addr-spec
               [";" CFWS report-format] CRLF

report-format = %s"report=" (%s"arf" / %s"xarf")
```

5.2. CFBL-Feedback-ID

The following ABNF imports the rules for fields, WSP, CRLF, and atext
from [RFC5322].

```
fields =/ cfbl-feedback-id

cfbl-feedback-id = "CFBL-Feedback-ID:" CFWS fid CRLF

fid = 1*(atext / ":" / CFWS)
```

Empty space is ignored in the fid value and MUST be ignored when
reassembling the original feedback-id.
In particular, the Message Originator can safely insert CFWS in the
fid value in arbitrary places to conform to line length limits when
adding the header field.

6. Security Considerations

This section discusses possible security issues of a CFBL-Address
header field and their solutions.

6.1. Attacks on the Feedback Loop Address

Like any other email address, a CFBL address can be an attack vector
for malicious messages. For example, CFBL addresses can be flooded
with spam. This is an existing problem with any existing email
address and is not created by this document.

6.2. Automatic Suspension of an Account

Receiving a Feedback Message regarding a Message Author can cause the
Message Author to be unreachable if an automatic account suspension
occurs too quickly. For example, someone sends an invitation to
their friends, and someone else marks this message as spam for some
reason.

If automatic account suspension is too fast, the Message Author's
account will be blocked and the Message Author will not be able to
access their emails or send further messages, depending on the
account suspension the Message Originator has chosen.

Message Originators must take appropriate measures to prevent account
suspensions that happen too fast. Therefore, Message Originators

have -- mostly proprietary -- ways to assess the trustworthiness of
an account. For example, Message Originators may take into account
the age of the account and/or any previous account suspension before
suspending an account.

6.3. Enumeration Attacks / Provoking Unsubscription

A malicious person may send a series of spoofed Abuse Reporting
Format (ARF) messages to known CFBL addresses and attempt to guess a
Message-ID / CFBL-Feedback-ID or any other identifiers. The
malicious person may attempt to mass unsubscribe/suspend if such an
automated system is in place. This is also an existing problem with
the current feedback loop implementation and/or One-Click
Unsubscription [RFC8058].

The Message Originator must take appropriate measures. For example,
the CFBL-Feedback-ID header field (if used) can use a hard-to-forge
component, such as an [HMAC] with a secret key, instead of a
plaintext string, to make an enumeration attack impossible.

6.4. Data Privacy

The provision of such a header field itself does not pose a data
privacy issue. The resulting ARF/XARF report sent by the Mailbox
Provider to the Message Originator may violate a data privacy law
because it may contain personal data.

This document already addresses some parts of this problem and
describes a way to send a Feedback Message that keeps data privacy
safe. As described in Section 3.5, the Mailbox Provider can omit the
entire body and/or header field and send only the required fields.
As recommended in [RFC6590], the Mailbox Provider can also redact the
data in question. Nevertheless, each Mailbox Provider must consider
for itself whether this implementation is acceptable and complies
with existing data privacy laws in their country.

As described in Sections 3.5 and 3.3, it is also strongly RECOMMENDED
that the Message-ID and CFBL-Feedback-ID (if used) contain a
component that is difficult to forge, such as an [HMAC] that uses a
secret key, rather than a plaintext string. See Section 8.3 for an
example.

6.5. Abusing for Validity and Existence Queries

This mechanism could be abused to determine the validity and
existence of an email address, exhibiting another potential data
privacy issue. If the Mailbox Provider has an automatic process to
generate a Feedback Message for a received message, it may not be
doing the mailbox owner any favors. As the Mailbox Provider
generates an automatic Feedback Message for the received message, the
Mailbox Provider proves to the Message Originator that this mailbox
exists for sure because it is based on a manual action of the mailbox
owner.

The receiving Mailbox Provider must take appropriate measures. One
possible countermeasure could be pre-existing reputation data

(usually proprietary data), for example. Using this data, the
Mailbox Provider can assess the trustworthiness of a Message
Originator and decide whether to send a Feedback Message based on
this information.

7. IANA Considerations

7.1. CFBL-Address

IANA has registered a new header field, per [RFC3864], in the
"Provisional Message Header Field Names" registry:

Header Field Name: CFBL-Address

Protocol: mail

Status:

Author/Change controller: Jan-Philipp Benecke <jpb@cleverreach.com>

Reference: RFC 9477

7.2. CFBL-Feedback-ID

IANA has registered a new header field, per [RFC3864], in the
"Provisional Message Header Field Names" registry:

Header Field Name: CFBL-Feedback-ID

Protocol: mail

Status:

Author/Change controller: Jan-Philipp Benecke <jpb@cleverreach.com>

Reference: RFC 9477

8. Examples

For simplicity, the DKIM header field has been shortened, and some
tags have been omitted.

8.1. Simple

Email about the report will be generated:

```
Return-Path: <sender@mailer.example.com>
From: Awesome Newsletter <newsletter@example.com>
To: me@example.net
Subject: Super awesome deals for you
CFBL-Address: fbl@example.com; report=arf
CFBL-Feedback-ID: 111:222:333:4444
Message-ID: <a37e51bf-3050-2aab-1234-543a0828d14a@mailer.example.com>
Content-Type: text/plain; charset=utf-8
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=news;
      h=Subject:From:To:Message-ID:CFBL-Feedback-ID:CFBL-Address;
```

This is a super awesome newsletter.

Resulting ARF report:

```
------=_Part_240060962_1083385345.1592993161900
Content-Type: message/feedback-report
Content-Transfer-Encoding: 7bit

Feedback-Type: abuse
User-Agent: FBL/0.1
Version: 0.1
Original-Mail-From: sender@mailer.example.com
Arrival-Date: Tue, 23 Jun 2020 06:31:38 GMT
Reported-Domain: example.com
Source-IP: 192.0.2.1

------=_Part_240060962_1083385345.1592993161900
Content-Type: text/rfc822; charset=UTF-8
Content-Transfer-Encoding: 7bit

Return-Path: <sender@mailer.example.com>
From: Awesome Newsletter <newsletter@example.com>
To: me@example.net
Subject: Super awesome deals for you
CFBL-Address: fbl@example.com; report=arf
CFBL-Feedback-ID: 111:222:333:4444
Message-ID: <a37e51bf-3050-2aab-1234-543a0828d14a@mailer.example.com>
Content-Type: text/plain; charset=utf-8
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=news;
      h=Subject:From:To:Message-ID:CFBL-Feedback-ID:CFBL-Address;

This is a super awesome newsletter.
------=_Part_240060962_1083385345.1592993161900--
```

8.2. Data Privacy Safe Report

Email about the report will be generated:

```
Return-Path: <sender@mailer.example.com>
From: Awesome Newsletter <newsletter@example.com>
To: me@example.net
Subject: Super awesome deals for you
CFBL-Address: fbl@example.com; report=arf
CFBL-Feedback-ID: 111:222:333:4444
Message-ID: <a37e51bf-3050-2aab-1234-543a0828d14a@mailer.example.com>
Content-Type: text/plain; charset=utf-8
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=news;
      h=Subject:From:To:Message-ID:CFBL-Feedback-ID:CFBL-Address;

This is a super awesome newsletter.
```

Resulting ARF report that only contains the CFBL-Feedback-ID:

```
------=_Part_240060962_1083385345.1592993161900
Content-Type: message/feedback-report
```

```
Content-Transfer-Encoding: 7bit

Feedback-Type: abuse
User-Agent: FBL/0.1
Version: 0.1
Original-Mail-From: sender@mailer.example.com
Arrival-Date: Tue, 23 Jun 2020 06:31:38 GMT
Reported-Domain: example.com
Source-IP: 2001:DB8::25

------=_Part_240060962_1083385345.1592993161900
Content-Type: text/rfc822-headers; charset=UTF-8
Content-Transfer-Encoding: 7bit

CFBL-Feedback-ID: 111:222:333:4444
------=_Part_240060962_1083385345.1592993161900--
```

8.3. Data Privacy Safe Report with HMAC

Email about the report will be generated:

```
Return-Path: <sender@mailer.example.com>
From: Awesome Newsletter <newsletter@example.com>
To: me@example.net
Subject: Super awesome deals for you
CFBL-Address: fbl@example.com; report=arf
CFBL-Feedback-ID: 3789e1ae1938aa2f0dfdfa48b20d8f8bc6c21ac34fc5023d
        63f9e64a43dfedc0
Message-ID: <a37e51bf-3050-2aab-1234-543a0828d14a@mailer.example.com>
Content-Type: text/plain; charset=utf-8
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=news;
        h=Subject:From:To:Message-ID:CFBL-Feedback-ID:CFBL-Address;

This is a super awesome newsletter.
```

Resulting ARF report that only contains the CFBL-Feedback-ID:

```
------=_Part_240060962_1083385345.1592993161900
Content-Type: message/feedback-report
Content-Transfer-Encoding: 7bit

Feedback-Type: abuse
User-Agent: FBL/0.1
Version: 0.1
Original-Mail-From: sender@mailer.example.com
Arrival-Date: Tue, 23 Jun 2020 06:31:38 GMT
Reported-Domain: example.com
Source-IP: 2001:DB8::25

------=_Part_240060962_1083385345.1592993161900
Content-Type: text/rfc822-headers; charset=UTF-8
Content-Transfer-Encoding: 7bit

CFBL-Feedback-ID: 3789e1ae1938aa2f0dfdfa48b20d8f8bc6c21ac34fc5023d
        63f9e64a43dfedc0
------=_Part_240060962_1083385345.1592993161900--
```

9. References

9.1. Normative References

[ARF]   Shafranovich, Y., Levine, J., and M. Kucherawy, "An
            Extensible Format for Email Feedback Reports", RFC 5965,
            DOI 10.17487/RFC5965, August 2010,
            <https://www.rfc-editor.org/info/rfc5965>.

[DKIM]   Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed.,
            "DomainKeys Identified Mail (DKIM) Signatures", STD 76,
            RFC 6376, DOI 10.17487/RFC6376, September 2011,
            <https://www.rfc-editor.org/info/rfc6376>.

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119,
            DOI 10.17487/RFC2119, March 1997,
            <https://www.rfc-editor.org/info/rfc2119>.

[RFC5234]   Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax
            Specifications: ABNF", STD 68, RFC 5234,
            DOI 10.17487/RFC5234, January 2008,
            <https://www.rfc-editor.org/info/rfc5234>.

[RFC5322]   Resnick, P., Ed., "Internet Message Format", RFC 5322,
            DOI 10.17487/RFC5322, October 2008,
            <https://www.rfc-editor.org/info/rfc5322>.

[RFC6449]   Falk, J., Ed., "Complaint Feedback Loop Operational
            Recommendations", RFC 6449, DOI 10.17487/RFC6449, November
            2011, <https://www.rfc-editor.org/info/rfc6449>.

[RFC6532]   Yang, A., Steele, S., and N. Freed, "Internationalized
            Email Headers", RFC 6532, DOI 10.17487/RFC6532, February
            2012, <https://www.rfc-editor.org/info/rfc6532>.

[RFC7405]   Kyzivat, P., "Case-Sensitive String Support in ABNF",
            RFC 7405, DOI 10.17487/RFC7405, December 2014,
            <https://www.rfc-editor.org/info/rfc7405>.

[RFC8174]   Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
            2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
            May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[XARF]   "XARF - eXtended Abuse Reporting Format", commit cc1a6e6,
            March 2023, <https://github.com/abusix/xarf>.

9.2. Informative References

[HMAC]   Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-
            Hashing for Message Authentication", RFC 2104,
            DOI 10.17487/RFC2104, February 1997,
            <https://www.rfc-editor.org/info/rfc2104>.

[RFC3864]   Klyne, G., Nottingham, M., and J. Mogul, "Registration

                   Procedures for Message Header Fields", BCP 90, RFC 3864,
                   DOI 10.17487/RFC3864, September 2004,
                   <https://www.rfc-editor.org/info/rfc3864>.

   [RFC6590]   Falk, J., Ed. and M. Kucherawy, Ed., "Redaction of
                   Potentially Sensitive Data from Mail Abuse Reports",
                   RFC 6590, DOI 10.17487/RFC6590, April 2012,
                   <https://www.rfc-editor.org/info/rfc6590>.

   [RFC8058]   Levine, J. and T. Herkula, "Signaling One-Click
                   Functionality for List Email Headers", RFC 8058,
                   DOI 10.17487/RFC8058, January 2017,
                   <https://www.rfc-editor.org/info/rfc8058>.

Acknowledgments

Author's Address

   Jan-Philipp Benecke
   CleverReach GmbH & Co. KG
   Schafjueckenweg 2
   26180 Rastede
   Germany
   Phone: +49 4402 97390-16
   Email: jpb@cleverreach.com