# Internal DFIR

Prepared for: Dallas Makerspace

Technical Resource: Jim Hartnett

| Document Revision | Date | Author |
|---|---|---|
| 1.0 | March 16, 2019 | Jim Hartnett |



HACKING & COFFEE
Security, Hosting, Wolf

# Table of Contents


1 Executive Summary ..... 3
2 Investigation Authorization ..... 4
3 Investigation Start & Incident Background ..... 5
4 Investigation Findings ..... 6
5 Core Investigation Findings ..... 6
5.1 The Source of the Original PureTax Email Sharing ..... 6
5.2 Disproving Robert Davidson's Knowledge of Email ..... 7
5.3 Andrew LeCody and Finance Group Work ..... 8
5.4 Verifying Statements Regarding PureTax "Approval" ..... 10
6 Appendix ..... 11
6.1 Second Email, as forwarded ..... 11
6.2 Email From Tim Halcomb Regarding Member Outreach ..... 12

Figure 1: G Suite Mail Log ..... 6
Figure 2: Robert Davidson Asking about Email *after* post ..... 7
Figure 3: Andrew LeCody Requesting QBO Access ..... 9
Figure 4: Andrew LeCody Sorting Expenses ..... 9
Figure 3: Except from PureTax Statement on Feb 21, 2019 ..... 10
Figure 4: Except from Talk post on Feb 12, 2019 from a BoD member ..... 10
Figure 5: Except from Talk post on Feb 12, 2019 from another BoD member ..... 10




HACKING & COFFEE
Security, Hosting, Wolf

# 1 Executive Summary

The Dallas Makerspace (DMS) engaged Jim Hartnett of Hacking & Coffee to perform a forensics investigation regarding leaked accounting firm information amongst their organization members. This investigation was performed on a best-effort, pro-bono basis at the behest of multiple parties to provide technical data supporting or disproving events and statements occurring on or about February 12, 2019.

**Full Disclosure:** It is important to note that the technical resources at the disposal of H&C, and its chief officer, are active DMS members. It was recommended that a different firm be hired for this matter to provide 3rd party validation of findings and processes, but this was rejected. All data is provided with screenshots, and methods of gathering as well as the scope of the particular search or analysis to mitigate internal biases.

During the course of the investigation various evidence was gathered, including that which indicated the following:

- Ken Purcell forwarded two emails to Andrew LeCody from PureTax
- Robert Davidson did not have knowledge of the PureTax email before the membership at large
- Andrew LeCody had at least some level of involvement with the finance group before the events took place
- The DMS board may not have received “thumbs up” by PureTax for any expansion plans

This report is not a matter of judgement nor does it recommend any actions against or for any members, but rather provides the results of a fact-finding operation from a technical perspective.



HACKING & COFFEE
Security, Hosting, Wolf

## 2 Investigation Authorization

After initial requests for data were fulfilled from previous incidents, and due to the conflicting nature of statements from all parties, H&C demanded a formal authorization for any investigation in which the contents of communications are reviewed.

This authorization was provided by the DMS Board of Directors on February 26, 2019

Link to official meeting minutes:
https://dallasmakerspace.org/wiki/Board_of_Directors_Meeting_20190226_Special_Meeting

Investigate Release of Dallas Makerspace Client Attorney privileged communications without authorizations
- Motion 4:
  Authorize forensic investigation to be conducted of Dallas Makerspace data/electronic media to determine source released privileged communication and report back to Board of Directors to determine any further actions.

- Proposed by David Kessinger
- Seconded by Steve Blanchard
- Call for vote
  - In favor unanimous
  - Opposed 0
  - Abstain 0
  - Motion Passed



HACKING & COFFEE
Security, Hosting, Wolf

# 3 Investigation Start & Incident Background

On February 12, 2019 Andrew LeCody posted a message on Talk indicating he had an internal email from PureTax as part of a discussion regarding DMS' plans for expansion, and whether accounting due diligence was being performed.

https://talk.dallasmakerspace.org/t/expansion-information/50756/59

In a subsequent reply, Andrew LeCody posted an excerpt from the email.

https://talk.dallasmakerspace.org/t/expansion-information/50756/61

The initial investigation was directed at three individuals to determine the source of the leaked PureTax email, and further determine if any other information was leaked and through what means.

Persons of Interest whose communications were subject to forensics:

- Ken Purcell
- Andrew LeCody
- Robert Davidson

The initial belief was that Ken Purcell had shared the email to Andrew LeCody and Robert Davidson through either their DMS email or through the TALK web forum. To test this notion, three technical methods were used by H&C to prove or disprove this initial notion and the order of events

- G Suite mail logs
- Talk Private Message (PM) search
- Google Takeout, with a Gmail target

G Suite mail logs provide easy to search metadata, whereas PM searches and Google Takeout provide relevant content to associated communications.

Statements made by the persons of interest also included information of impropriety that led to the release of data, and that such statements should be considered exculpatory if true. Data related to such statements are included in this report.



HACKING & COFFEE
Security, Hosting, Wolf

# 4 Investigation Findings

Below is a list of technical findings

| Section | Finding |
|---|---|
| 5.1 | The Source of the Original PureTax Email Sharing |
| 5.2 | Disproving Robert Davidson's Knowledge of Email |
| 5.3 | Andrew LeCody and Finance Group Work |
| 5.4 | Verifying Statements Regarding PureTax "Approval" |

# 5 Core Investigation Findings

## 5.1 The Source of the Original PureTax Email Sharing

Through G Suite mail logs, H&C was able to determine that Ken Purcell forwarded the puretax email from his DMS provided email to Andrew LeCody's personal Gmail account on February 12, 2019.

### TECHNICAL METHODS:

- G SUITE MAIL LOGS
  - SEARCH BY EMAIL SUBJECT
  - SEARCH BY RECIPIENT

### EVIDENCE

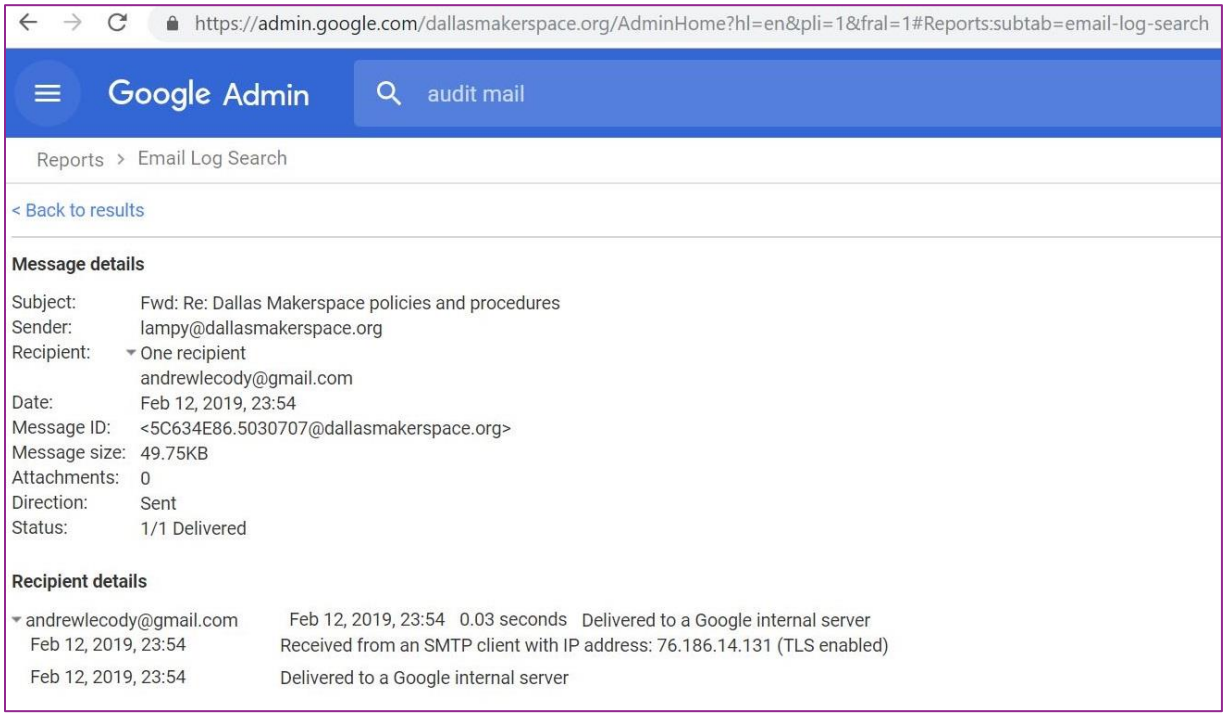



*Figure 1: G Suite Mail Log*



HACKING & COFFEE
Security, Hosting, Wolf

## 5.2 Disproving Robert Davidson's Knowledge of Email

After the initial email forward, the investigation continued to determine whether the email was known by others besides Andrew LeCody and Ken Purcell before the associated talk disclosure. The person of interest identified by the DMS Board of Directors as likely having knowledge is Robert Davidson.

All technical data recovered indicates that Robert Davidson did not have knowledge of the email contents before he Talk post and was uninvolved in the situation. Additionally, no email logs indicate forwarding of internal emails.

Exculpatory evidence is provided below to justify this negative finding.

### TECHNICAL METHODS:

- TALK PM AUDIT
  - PM REVIEW OF ANDREW LECODY ACCOUNT
  - PM REVIEW OF KEN PURCELL ACCOUNT
- G SUITE LOGS
  - SEARCH BY EMAIL SUBJECT
  - SEARCH BY RECIPIENT

The screenshot below was taken on February 27, 2019 (15 days after the talk disclosure).

### EVIDENCE

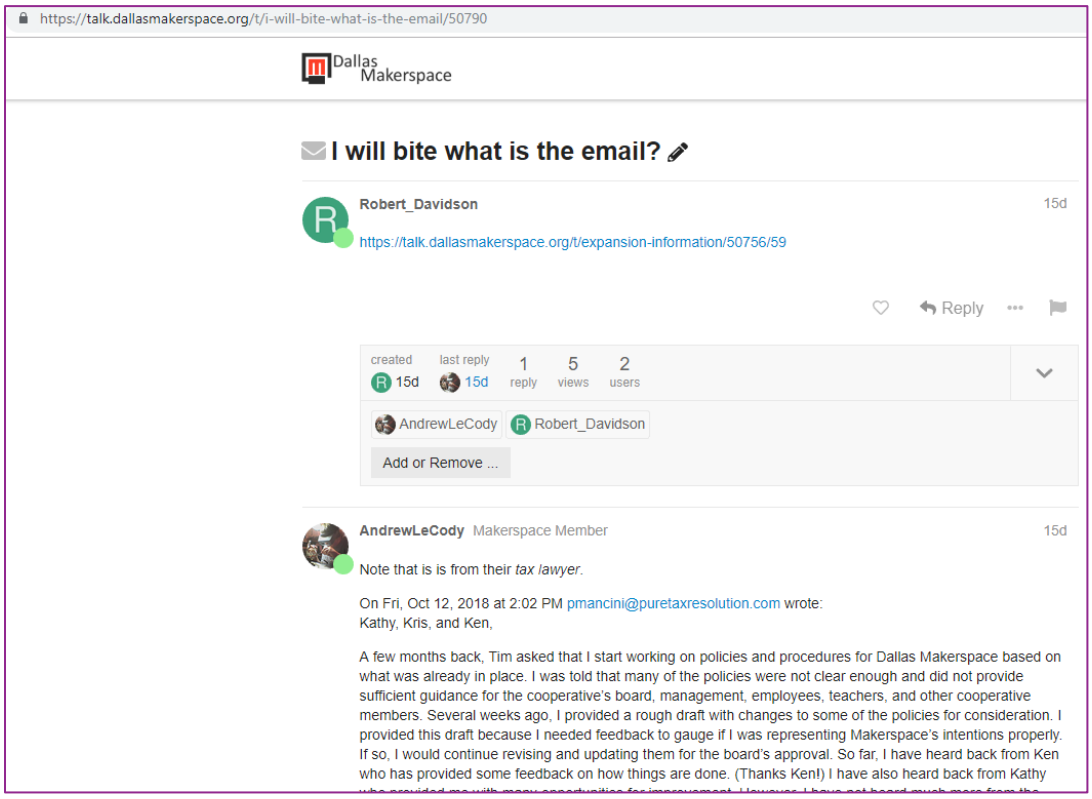



*Figure 2: Robert Davidson Asking about Email *after* post*



HACKING & COFFEE
Security, Hosting, Wolf

## 5.3 Andrew LeCody and Finance Group Work

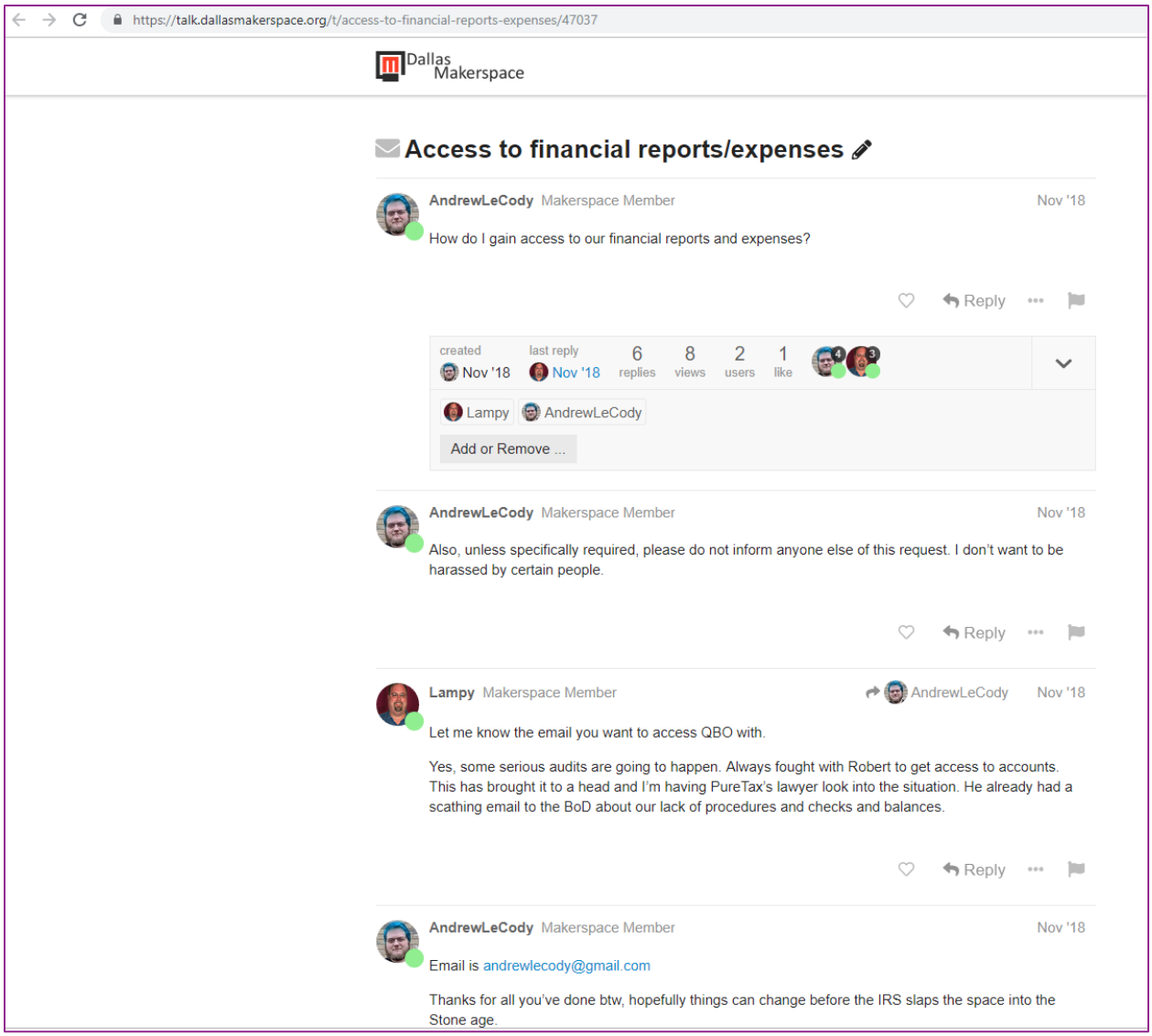
A statement was made regarding Andrew LeCody's involvement or assistance in financial group work before the events of February 12, 2019. One facet of this investigation is to determine if Andrew LeCody was in fact working with the finance group as part of any internal efforts at DMS and, as such, was privy to the associated background information at the time.

Given the nature of the requests and use of non-DMS communications media, it is not possible to determine the full nature of involvement outside of these messages.

### TECHNICAL METHODS:

- **TALK PM AUDIT**
  - **PM REVIEW OF ANDREW LECODY ACCOUNT**
  - **PM REVIEW OF KEN PURCELL ACCOUNT**

### EVIDENCE






HACKING & COFFEE
Security, Hosting, Wolf

*Figure 3: Andrew LeCody Requesting QBO Access*

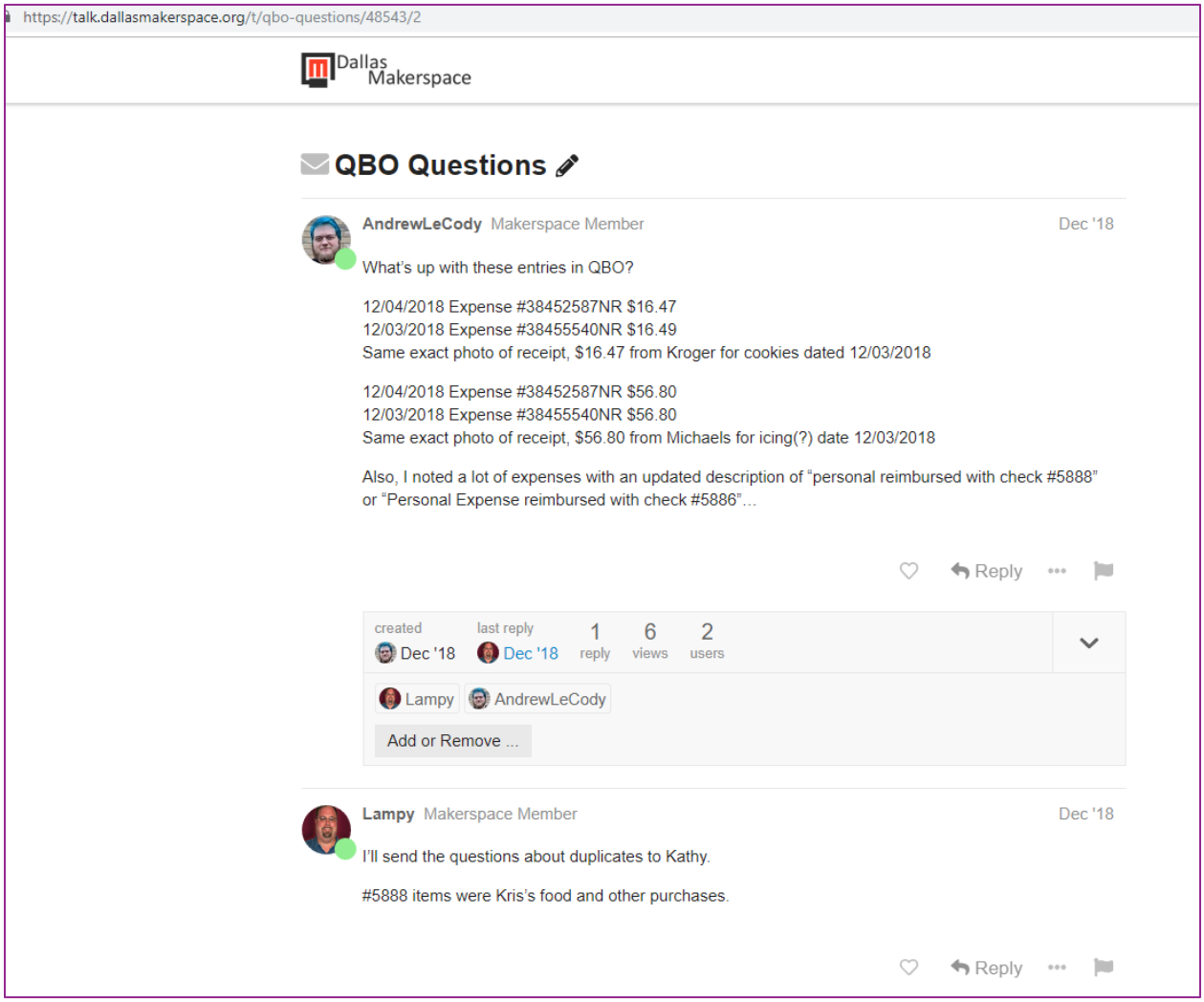



*Figure 4: Andrew LeCody Sorting Expenses*



HACKING & COFFEE
Security, Hosting, Wolf

## 5.4 Verifying Statements Regarding PureTax "Approval"

Contrary to what had been stated by board members at meetings and on the Talk forum, PureTax sent emails indicating they did not approve / "green light" any expansion plans.

This was requested to be included in the investigation by multiple anonymous parties, as many actions undertaken by the membership allegedly stem from the stance PureTax has taken with respect to certain plans made by DMS.

Whilst H&C will not make determinations on member actions, this information is provided for the record.

**RELATED POSTS AND/OR STATEMENTS:**

1. https://talk.dallasmakerspace.org/t/expansion-information/50756
2. https://talk.dallasmakerspace.org/t/expansion-information/50756/28
3. https://talk.dallasmakerspace.org/t/expansion-information/50756/36
4. https://talk.dallasmakerspace.org/t/expansion-information/50756/59
5. https://talk.dallasmakerspace.org/t/expansion-information/50756/60

**TECHNICAL METHODS:**

- **G SUITE LOGS**
  - **SEARCH MESSAGES FROM** thalcomb@puretaxresolution.com **ON FEB 21, 2019**
- **GOOGLE TAKEOUT**

**EVIDENCE**

> *Specifically, I am aware of statements that were made claiming the Pure Tax, or its employees, have endorsed action plans that it never had. These claims were used to move personal agendas forward by trying to validate personal positions with our support that did not exist.*

*Figure 5: Except from PureTax Statement on Feb 21, 2019*

> Meanwhile, we have the blessing from our Expansion Committee as well as our accounting firm. No red flags from either. Except, get the contract signed with the contractor.

*Figure 6: Except from Talk post on Feb 12, 2019 from a BoD member*

> This has put the entire expansion project in jeopardy and we have all worked too hard to have it go down the drain. We have the money to make this a reality and have gotten a thumbs up from our accounting firm.

*Figure 7: Except from Talk post on Feb 12, 2019 from another BoD member*



HACKING & COFFEE
Security, Hosting, Wolf

# 6 Appendix

## 6.1 Second Email, as forwarded

Here is what I received from Tim @ PureTax:

*To All,*

*I am writing this note to follow up with the board meeting and recent events. I am having the questions you submitted reviewed by Peter Mancini in our office. I have ask that he get this completed as soon as possible to complete the SOP for your review and approval. In moving forward we will include all members of the BOD, accounting and treasurer in these emails. In preparation for an upcoming audit I request that you all be very clear as to financial documentation and expenditures. The BOD of Directors and Treasurer as they stand today are all responsible for the finances of DMS. With this said, in order to protect DMS from any issues within an audit we are going to request Kathy communicate all details of transactions and match them up with the person and person(s) responsible. There should not be any transactions hidden and all transparent for review.*

*I appreciate that you are all going through a difficult time. If you should choose to make any changes in BOD's or a treasurer please let us know as soon as possible. We will require a suitable replacement to work with Kathy to make sure the accounting is done correctly and accurately. In preparation for moving forward we will document everything for the incoming board so there is no question as to how we go to this point. If this email is unclear or you would like us to schedule a call to go into greater detail please feel free to let me know.*

*Regards,*

*Tim*

***Timothy C. Halcomb***

***President/CEO***

***Pure Tax Resolution***
***(800) 462-7021 Phone***
***(866) 322-0970 Fax***
*Email:* *thalcomb@puretaxresolution.com*

*Website:* *PureTaxHelp.com*



HACKING & COFFEE
Security, Hosting, Wolf

## 6.2 Email From Tim Halcomb Regarding Member Outreach

Dallas Makerspace board of directors:

I am writing today to share with you my thoughts and observations from things that have been happening at Dallas Makerspace (DMS) recently that have impacted Pure Tax Resolution directly. Specifically, I want to address recent actions of DMS's officers and some board members that call into question their commitment to proper cooperative governance. I will start with that I have been contacted by members, officers, board members (current and past), DMS staff, and my employee over the past month recounting dubious ethical behavior by many at DMS. I was told about misrepresentations and lies that were stated to manipulate DMS to take certain actions. Specifically, I am aware of statements that were made claiming the Pure Tax, or its employees, have endorsed action plans that it never had. These claims were used to move personal agendas forward by trying to validate personal positions with our support that did not exist. Further, I have been told about dubious board-member and officer actions that were directed at Pure Tax employees. Specifically, Pure Tax employees were told not to disclose financial information (e.g. DMS's expenses and commitments to expend DMS's money) with DMS's treasurer. By making these statements and taking these actions, DMS is prohibiting Pure Tax and its employees from doing what it had been contracted to do. All this must stop immediately!

Board members are entrusted to represent a cooperative's best interests. To determine what is in a cooperative's best interests, its board should engage in the free flow of information and ideas then consider different options and opinions at a board level. Only after that process, can an informed decision for the cooperative be rendered. Failing to do so shows that a board is not making informed, business decisions that are in a cooperative's best interest. And that is what I am seeing here.

Further, for a cooperative to be successful, its members must know what it happening. In the past weeks, I have been bombarded with separate contacts from DMS officers, board members, and members about issues that were to be kept secret, issues that I was not to share with select people, or issues that Pure Tax employees were not able to share at all. This has put me and my employees in a very precarious position. Pure Tax Resolution represents Dallas Makerspace. It does not represent a board member, an officer, or a member. Consequently, my firm has been charged to do what is in the best interests of the cooperative and not what is in the best interest of one or a few people who are part of Dallas Makerspace. So for my firm to meet its commitments, this too must stop!

Last, we have seen, and documented, instances where misrepresentations and down-right lies have been stated about Pure Tax endorsing on plan or another. We have seen, and documents, instances where personal agendas are being moved forward – at membership expense – without regard to long-term viability where we have been asked to be complicit. Then we have seen, and documented, instances where there is no free flow of information, ideas are stifled, viable options are not considered, and opposing opinions are not heard by its board. We have seen, and documented, dubious decisions and actions taken by some board members and DMS's officers that are not in DMS's best interest. And we have seen many instances where members, officers, or board members have exceeded their authorities, as we know them, after claims were made the Pure Tax had approved these actions when Pure Tax had not. For Pure Tax to continue working with DMS, this must stop because it is wholly unacceptable!



HACKING & COFFEE
Security, Hosting, Wolf

For Pure Tax and DMS to move forward working together through a renewed services agreement, there must be immediate change. Clearly-stated, board-set policies must be determined and adopted by DMS's board. DMS's board, officers, and its members must all agree to and actually abide by its own policies. And these policies must be shared – in whole – with Pure Tax, so we know what DMS deems to be acceptable and not acceptable. If after reviewing DMS's policies – specifically ones that address authorities to expend money, the approval processes, and the checks and balances that will be in place – Pure Tax is not satisfied that it is being provided adequate guidance, our relationship will end immediately.

Should our relationship end, Kathy (Pure Tax's employee and DMS's on-site bookkeeper) will be recalled immediately, and we will begin an orderly exit. This will include drafting a closing report that will comprehensively document what happen and why this relationship had to end. It will be made available and shared with all, so Pure Tax can explain to DMS's membership that it was working in the cooperative's best interests despite its leadership's actions. Then I expect that DMS will take over all accounting and bookkeeping immediately.

Pure Tax will need an answer from DMS's board very soon. I expect to hear a response within the next week, so by February 28, 2019, I know where we stand. If no formal written answer is provided by then, our relationship will end. So put simply, I am seeking DMS's board to commit to what it expected of them: its existing fiduciary duties and proper cooperative governance. Then, if we are all in agreement, I will arrange for a new service agreement to be drafted that memorializes all this. DMS's board will then consider it and approve it, as a whole, unanimously.

If this is coming as a surprise to some DMS board members, I am sorry. To be clear, I am not trying to ambush anyone because I am under the impression that the DMS board has been privy to all that goes on there. But finding out that there are these problems through this email further enforces what we have been observing.

I now await your response. The DMS board must provide me that response by February 28, 2019, 5:00 PM EST.

Regards,

***Timothy C. Halcomb***
***President/CEO***

***Pure Tax Resolution***
***(800) 462-7021 Phone***
***(866) 322-0970 Fax***
*Email:* *thalcomb@puretaxresolution.com*
*Website:* *PureTaxHelp.com*



HACKING & COFFEE
Security, Hosting, Wolf