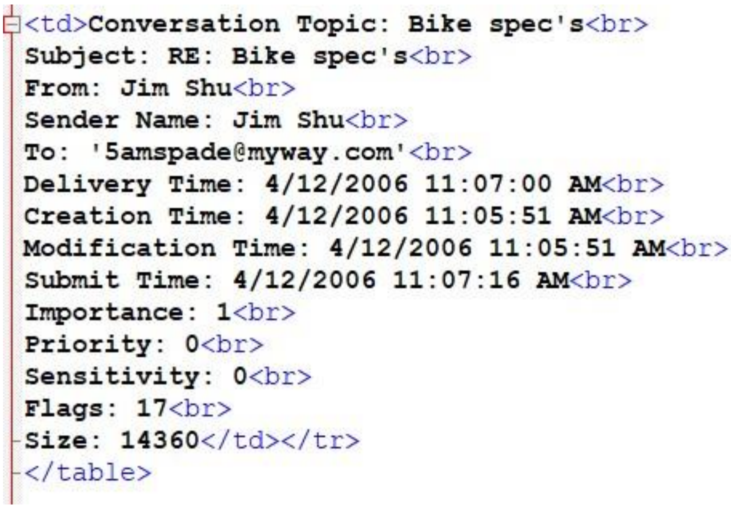
Muhammad Izham Bin Norhamadi
B032020039

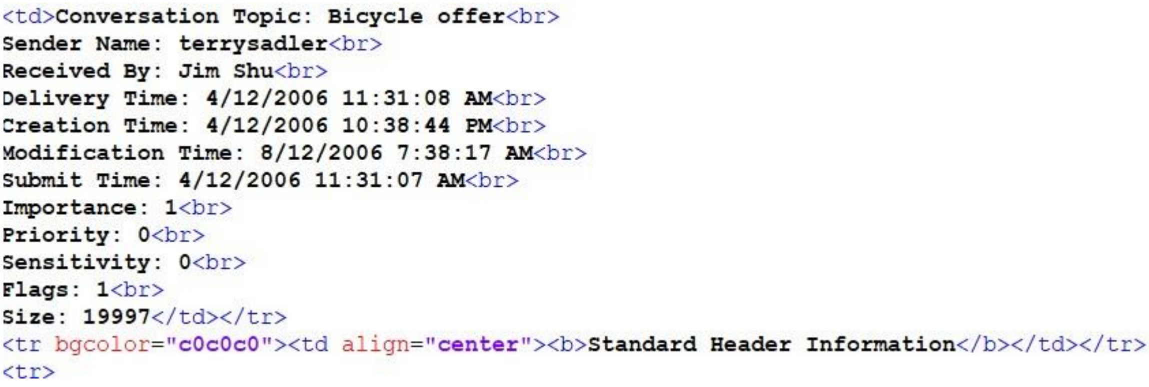
Lab 12

Task 1

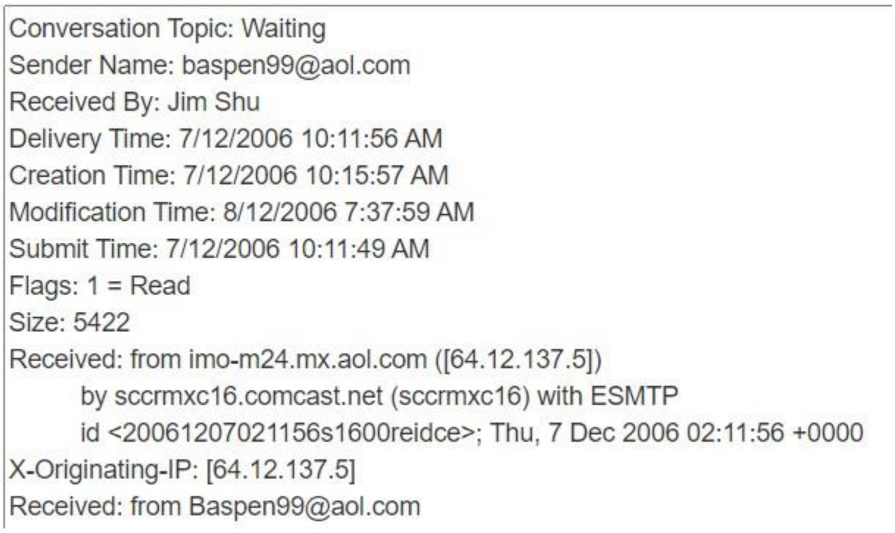
From the keyword search Cash and Money, we receive 16 hits from 8 files. The conversations circles around 4 person, Sam (5amspade@myway.com), Jim Shu (Jim_shu@comcast.net), terrysadler (terrysadler@goowy.com), and Bob (baspen99@aol.com).



```
<td>Conversation Topic: Bike spec's<br>
Subject: RE: Bike spec's<br>
From: Jim Shu<br>
Sender Name: Jim Shu<br>
To: '5amspade@myway.com'<br>
Delivery Time: 4/12/2006 11:07:00 AM<br>
Creation Time: 4/12/2006 11:05:51 AM<br>
Modification Time: 4/12/2006 11:05:51 AM<br>
Submit Time: 4/12/2006 11:07:16 AM<br>
Importance: 1<br>
Priority: 0<br>
Sensitivity: 0<br>
Flags: 17<br>
Size: 14360</td></tr>
</table>
```



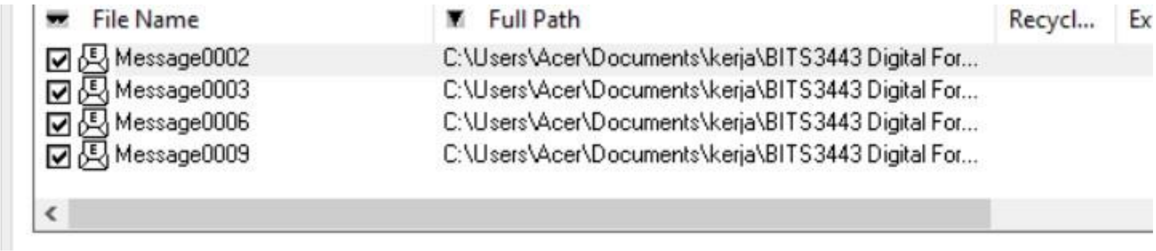
```
<td>Conversation Topic: Bicycle offer<br>
Sender Name: terrysadler<br>
Received By: Jim Shu<br>
Delivery Time: 4/12/2006 11:31:08 AM<br>
Creation Time: 4/12/2006 10:38:44 PM<br>
Modification Time: 8/12/2006 7:38:17 AM<br>
Submit Time: 4/12/2006 11:31:07 AM<br>
Importance: 1<br>
Priority: 0<br>
Sensitivity: 0<br>
Flags: 1<br>
Size: 19997</td></tr>
<tr bgcolor="c0c0c0"><td align="center"><b>Standard Header Information</b></td></tr>
<tr>
```



```
Conversation Topic: Waiting
Sender Name: baspen99@aol.com
Received By: Jim Shu
Delivery Time: 7/12/2006 10:11:56 AM
Creation Time: 7/12/2006 10:15:57 AM
Modification Time: 8/12/2006 7:37:59 AM
Submit Time: 7/12/2006 10:11:49 AM
Flags: 1 = Read
Size: 5422
Received: from imo-m24.mx.aol.com ([64.12.137.5])
        by sccrmxc16.comcast.net (sccrmxc16) with ESMTP
        id <20061207021156s1600reidce>; Thu, 7 Dec 2006 02:11:56 +0000
X-Originating-IP: [64.12.137.5]
Received: from Baspen99@aol.com
```

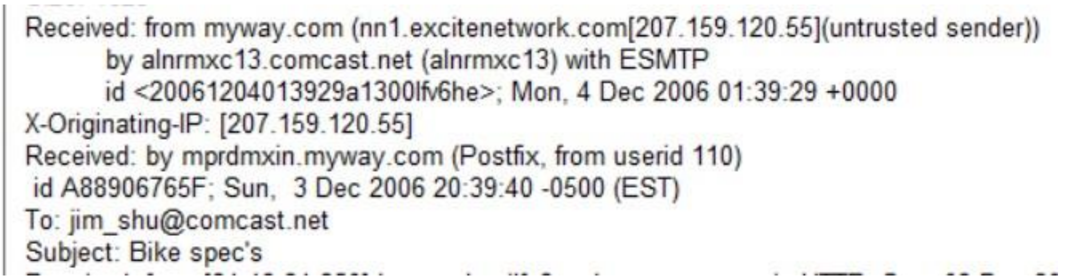
Task 2

From investigation of similar ids between emails, 4 email headers were added Anti Abuse ID that were sent from untrusted sender. The emails are from Sam to Jim Shu.



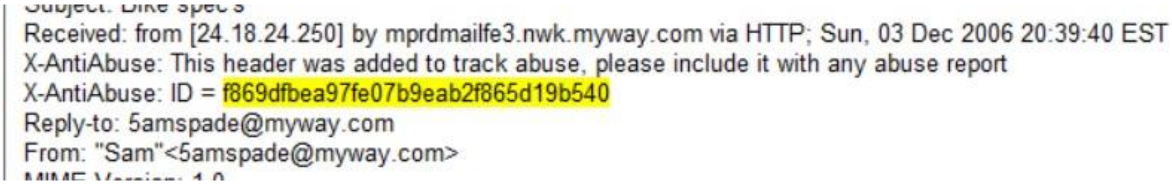
File Name	Full Path	Recycl...	Ex
☑ Message0002	C:\Users\Acer\Documents\kerja\BITS3443 Digital For...		
☑ Message0003	C:\Users\Acer\Documents\kerja\BITS3443 Digital For...		
☑ Message0006	C:\Users\Acer\Documents\kerja\BITS3443 Digital For...		
☑ Message0009	C:\Users\Acer\Documents\kerja\BITS3443 Digital For...		

Message header from Bike spec’s



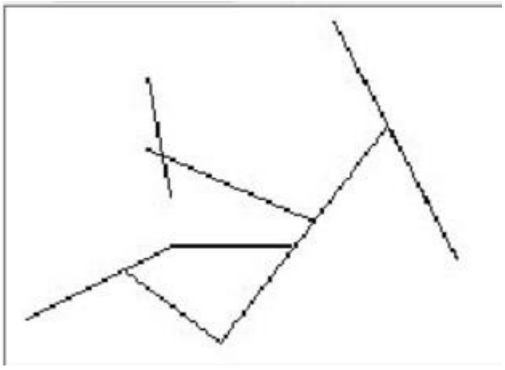
```
Received: from myway.com (nn1.excitenetwork.com[207.159.120.55](untrusted sender))
        by alnrmxc13.comcast.net (alnrmxc13) with ESMTP
        id <20061204013929a1300lfv6he>; Mon, 4 Dec 2006 01:39:29 +0000
X-Originating-IP: [207.159.120.55]
Received: by mprdmxin.myway.com (Postfix, from userid 110)
 id A88906765F; Sun,  3 Dec 2006 20:39:40 -0500 (EST)
To: jim_shu@comcast.net
Subject: Bike spec's
```

X-AntiAbuse ID

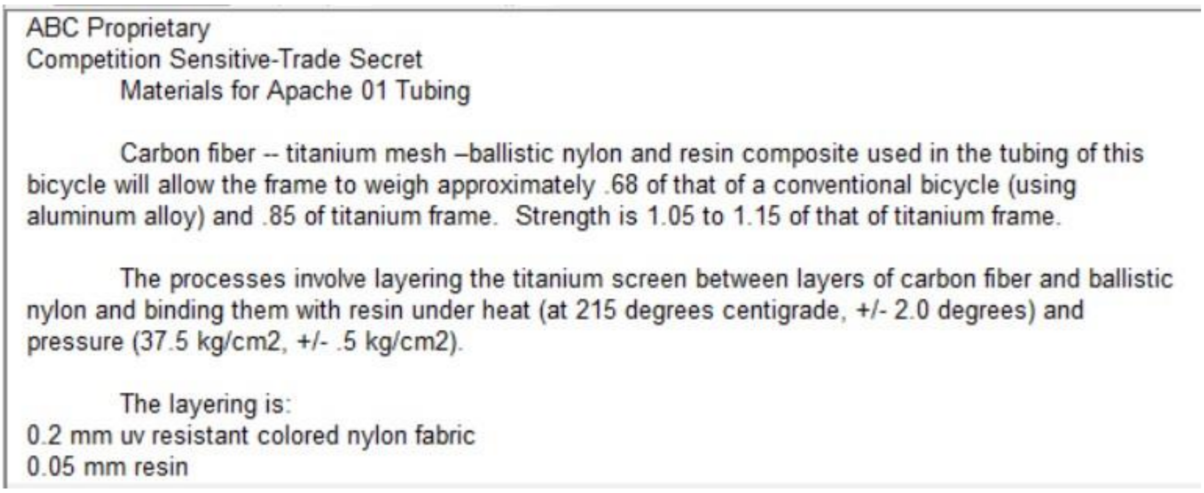


Received: from [24.18.24.250] by mprdmailfe3.nwk.myway.com via HTTP; Sun, 03 Dec 2006 20:39:40 EST
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: ID = f869dfbea97fe07b9eab2f865d19b540
Reply-to: 5amspade@myway.com
From: "Sam"<5amspade@myway.com>

There are two forwarded message which are Message0007 and Message0008 from Inbox. Message0001 and Message0002 were created for the email forwarding and were deleted and are now in Deleted Items. “AC19.gpf” and “Tubing Materials.rtf” are the attached files.



AC19.gpf



ABC Proprietary
Competition Sensitive-Trade Secret
Materials for Apache 01 Tubing

Carbon fiber -- titanium mesh –ballistic nylon and resin composite used in the tubing of this bicycle will allow the frame to weigh approximately .68 of that of a conventional bicycle (using aluminum alloy) and .85 of titanium frame. Strength is 1.05 to 1.15 of that of titanium frame.

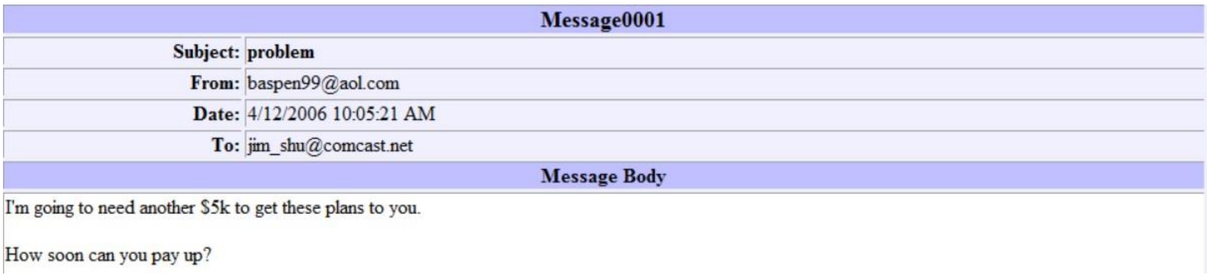
The processes involve layering the titanium screen between layers of carbon fiber and ballistic nylon and binding them with resin under heat (at 215 degrees centigrade, +/- 2.0 degrees) and pressure (37.5 kg/cm2, +/- .5 kg/cm2).

The layering is:
0.2 mm uv resistant colored nylon fabric
0.05 mm resin

Tubing Materials.rtf

Task 3

There are 8 deleted items, the two attachments previously and Message0001, Message0002 Message0007, Message0008, Message0009 and Message0010. Only Message0002 is from terrysadler, the rest are from Bob.

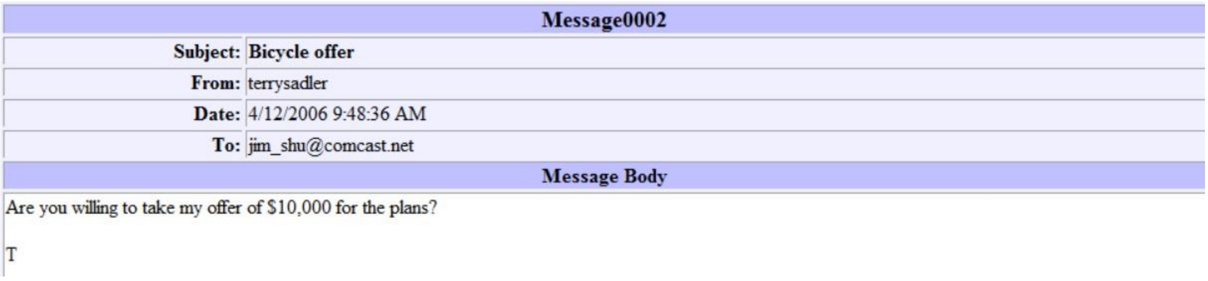


Message0001	
Subject:	**problem**
From:	baspen99@aol.com
Date:	4/12/2006 10:05:21 AM
To:	jim_shu@comcast.net

Message Body

I'm going to need another $5k to get these plans to you.

How soon can you pay up?

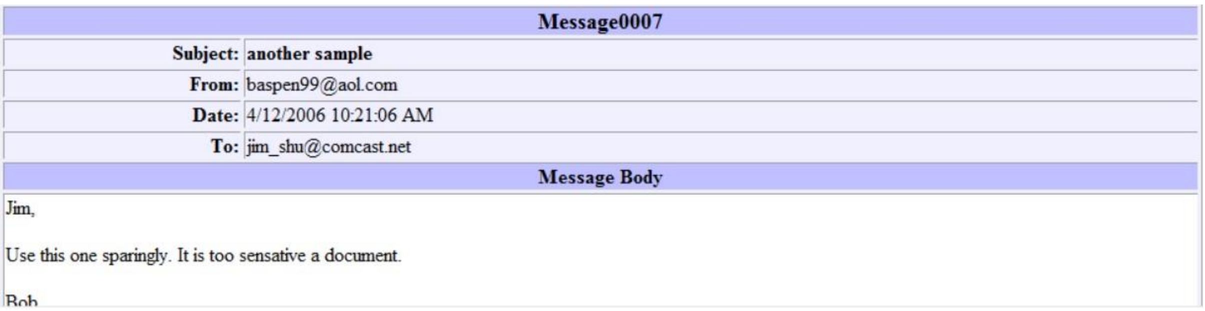


Message0002	
Subject:	**Bicycle offer**
From:	terrysadler
Date:	4/12/2006 9:48:36 AM
To:	jim_shu@comcast.net

Message Body

Are you willing to take my offer of $10,000 for the plans?

T



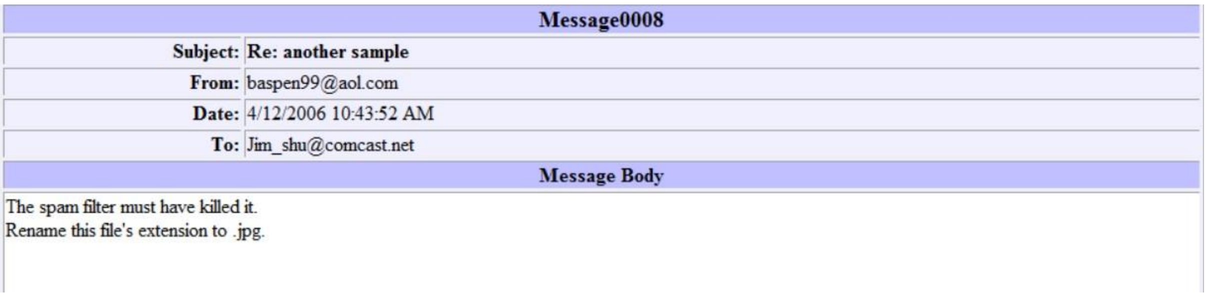
Message0007	
Subject:	**another sample**
From:	baspen99@aol.com
Date:	4/12/2006 10:21:06 AM
To:	jim_shu@comcast.net

Message Body

Jim,

Use this one sparingly. It is too sensative a document.

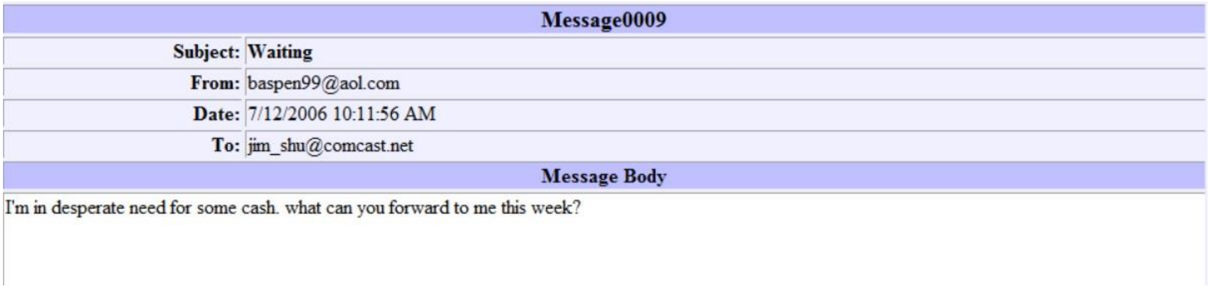
Bob



Message0008	
Subject:	**Re: another sample**
From:	baspen99@aol.com
Date:	4/12/2006 10:43:52 AM
To:	Jim_shu@comcast.net

Message Body

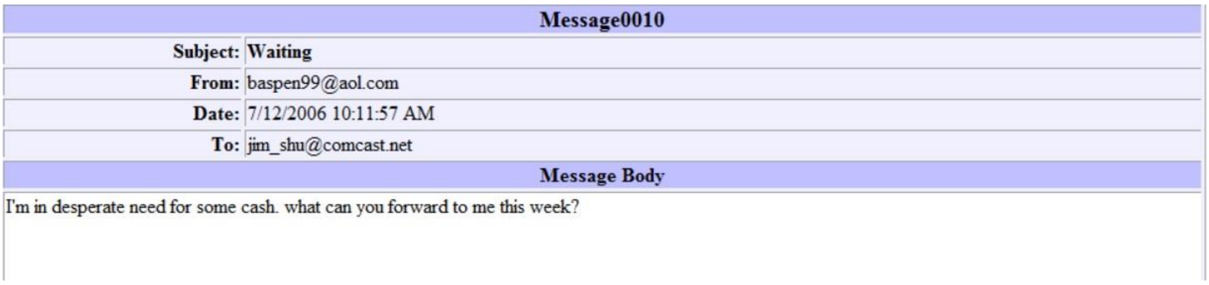
The spam filter must have killed it.
Rename this file's extension to .jpg.



Message0009	
Subject:	**Waiting**
From:	baspen99@aol.com
Date:	7/12/2006 10:11:56 AM
To:	jim_shu@comcast.net

Message Body

I'm in desperate need for some cash. what can you forward to me this week?



Message0010	
Subject:	Waiting
From:	baspen99@aol.com
Date:	7/12/2006 10:11:57 AM
To:	jim_shu@comcast.net
Message Body	
I'm in desperate need for some cash. what can you forward to me this week?	

Task 4

From the Internet keyword search, goowy.com is a commonly used email domain and address. Other email domain used are comcast.net, yahoo.com and aol.com. excitenetwork.com is an untrusted sender and is marked with X-AntiAbuse header. Email footers occasionally have an ad for myway.com.

Task 5

```
From martha.dax@superiorbicycles.biz Wed Feb 14 18:05:26 2007
Subject: Audits
From: Martha Dax <martha.dax@superiorbicycles.biz>
To: Chris.murphy@superiorbicycles.biz
Cc: robert.swartz@superiorbicycles.biz
Content-Type: text/plain
Message-Id: <1171504991.8622.3.camel@localhost.localdomain>
Mime-Version: 1.0
X-Mailer: Evolution 2.8.2.1 (2.8.2.1-3.fc6)
Content-Transfer-Encoding: 7bit
Date: Wed, 14 Feb 2007 18:05:26 -0800
X-Evolution-Format: text/plain
X-Evolution-Account: 1171494977.8622.20@Mapel06
X-Evolution-Transport:
        smtp://martha.dax;auth=PLAIN@smtp.superiorbicycles.biz/;use_ssl=never
X-Evolution-Fcc: mbox:/home/martha/.evolution/mail/local#Sent
X-Evolution: 00000002-0010

Chris,

We will need to prepare for the annual board meeting. Can you coordinate
with Bob those special projects?

Martha
```

```
From martha.dax@superiorbicycles.biz Wed Feb 14 18:18:11 2007
Subject: Re: New Product Development
From: Martha Dax <martha.dax@superiorbicycles.biz>
To: Jim Shu <jim.shu@superiorbicycles.biz>
In-Reply-To: <1b5698a2329b3dc9e557394f3a74f916@superiorbicycles.biz>
References: <1170648496.28879.9.camel@localhost.localdomain>
          <1b5698a2329b3dc9e557394f3a74f916@superiorbicycles.biz>
Content-Type: text/plain
Message-Id: <1171505889.8622.5.camel@localhost.localdomain>
Mime-Version: 1.0
X-Mailer: Evolution 2.8.2.1 (2.8.2.1-3.fc6)
Content-Transfer-Encoding: 7bit
Date: Wed, 14 Feb 2007 18:18:11 -0800
X-Evolution-Format: text/plain
X-Evolution-Account: 1171494977.8622.20@Mapel06
X-Evolution-Transport:
         smtp://martha.dax;auth=LOGIN@smtp.superiorbicycles.biz/;use_ssl=never
X-Evolution-Fcc: mbox:/home/martha/.evolution/mail/local#Sent
X-Evolution: 00000004-0010

Jim,

No date, we need to keep this as private as possible for the broad to
review.

Don't tell anyone about it!

Martha

On Wed, 2007-02-14 at 20:11 -0600, Jim Shu wrote:
> Martha, will this be available for public release soon? Jim
>
> On Feb 4, 2007, at 10:08 PM, Martha Dax wrote:
>
> >  Hello everybody!
> >
> >  We have a new announcement to make that is very sensitive regarding a
> > new business venture for us. It is the manufacturing of Kayaks in
> > addition to our bicycle line of products. Our advertising people are
> > excited about this new addition to our line of fine products.
> >
> >  For security purposes this is competitive sensitive information. Do
> > not tell anyone outside our executive staff about this new
```

> > development.
> >
> > Regards,
> > --
> > Martha Dax, CEO
> > Superior Bicycles, LLC
> > <PICT0032.JPG><PICT0059.JPG>

From: "Martha Dax" <martha.dax@superiorbicycles.biz>
To: <Chris.murphy@superiorbicycles.biz>
Cc: <robert.swartz@superiorbicycles.biz>
Sent: Wednesday, February 14, 2007 6:03 PM
Subject: Audits

> Chris,
>
> We will need to prepare for the annual board meeting. Can you coordinate
> with Bob those special projects?
>
> Martha
>