Fraud Identification and Prevention

Jonathan Lyon
Tax Technology and Standards
FTA

Good morning and my thanks to Commissioner Sullivan and his staff for allowing me to join you.

Before reviewing the various fraud prevention efforts underway, I'd like to spend a little time on the current environment in which Identity Theft takes place.

Then move into our joint work with Industry and IRS, and allow time for questions.

- **You Are The Product**
- **Identity Theft**
- **FTA Efforts**
- **IRS-States-Industry Summit**
- **Questions**

Fraud Identification and Prevention

- Oh, Do We Share
- Identity Theft
- FTA Efforts
- IRS-States-Industry Summit
- Questions

NESTOA 2015 2

First –
Some speakers start with a joke, but I'd like to begin with a personal story:

It's one I used at the FTA Annual Meeting in June, so forgive me if you've heard it before. As a member of the Baby Boom generation, I was always taught to protect my social security number, and in particular to secure the physical card in a safe place. So I've kept my family's cards in a safe deposit box along with other important personal documents, like our wills and advance medical directives.

I was reminded of this when my son called recently - he had started a new job - and said he needed his card for Human Resources Department processing at his new employer; and of course I provided it to him, and then I thought - what a quaint practice it is to exercise such caution over a paper card, when our personal data is increasingly available to malefactors over the Internet.

Who among us does not have a connection to someone who has experienced a compromise of a payment card, or their identity, or at least been the subject of a phishing call or e-mail purporting to be from IRS.

My wife is an Assistant U.S. Attorney, and a friend and someone that she works with closely, a counterpart in the United States Public Defender's Office, had her identity stolen and a tax return filed during this filing season.

As I'm sure we all understand, my wife's colleague was very upset, and also did not understand why it is so difficult to deal with and to get information from the government about her situation. On average it takes from 6 to 12 months to address an ID theft situation, and often very much longer.

That experience is being repeated a thousand times over, and more, across America.

That was in February.

Fraud Identification and Prevention

- Oh, Do We Share
- Identity Theft
- FTA Efforts
- IRS-States-Industry Summit
- Questions

NESTOA 2015 3

Since that time, our family has learned that my wife's records were among those stolen in the Office of Personnel Management incident – one among 21 million.

Then, about 4 weeks after being notified of that, my 29-year old daughter received a letter in the mail from OPM – 10 years after she had done an internship in my wife's office as a college sophomore - and her background check records were also among those compromised.

Add to that, that as a beneficiary under the Affordable Care Act she is an Empire Blue Cross/Blue Shield customer – which is owned by Anthem Health Care – of the 80-million-personal-records-breached Anthem.

So both my daughter and wife are now the beneficiaries of identity protection services, courtesy of the federal government.

I guess I should feel better, for that … but last then Thursday, the news was that instead of the 1.1 million fingerprint records stolen in the OPM breach, the number was actually 5.6 million.

I'll come back to the topic of biometrics.

Recent Press Release

Congress today re-authorized funding for Facebook, the massive online surveillance program run by the CIA. According to reports, Facebook has replaced almost every other CIA information – gathering program since it was launched in 2004.

"After years of secretly monitoring the public, we were astounded so many people would willingly publicize where they live, their religious and political views, an alphabetized list of all their friends, their e-mail addresses, phone numbers, hundreds of photos of themselves, and even updates on what they were doing at that moment.

It is truly a dream come true. Much of the credit belongs to CIA agent Mark Zuckerberg, who runs the day-to-day operation."

(Actually from The Onion News Network)

NESTOA 2015 4

Thousands of press releases are issued daily, but here's one that caught my eye:

(Actually from The Onion News Network)

It's funny – and not as un-funny as it should be.

Catch Me Now

"What I did in my youth is hundreds of times easier today."

- Frank Abagnale

NESTOA 2015 5

Many of you may remember that Frank Abagnale, the subject of the movie Catch Me If You Can, was the keynote speaker at the 2014 FTA Annual Meeting.

There probably is not a more qualified person to comment on identity theft out there. So his comment is cogent.

But what can be done on the Internet makes the kind of activities he engaged in look like child's play.

Identity Theft
(Your Numbers May Vary)

- 2012: (Congr Research Svc)
- ID Theft cost Americans $25B
- 17M victims, more than one every 2 seconds
- Overall costs $100B

NESTOA 2015 6

According to the Federal Trade Commission, tax identity theft has been the largest ID theft category for the last five years.

Reportedly, as of 2012, ID Theft cost Americans $25B,

Claiming 17M victims, more than one every 2 seconds,

With overall costs, Direct and Indirect, of $100B.

IRS tells us that they prevented $15B in fraud in 2015 – but lost an estimated $5B – and it's hard not to think that recent state numbers, in the aggregate, may not vary from that figure much.

Oh, Do We Share

2014 – During Every Minute, of Every Day, We:

- Sent 204M e-mails
- Shared 684K posts on Facebook
- Posted 36K pictures on Instagram
- Sent 100k tweets on Twitter

NESTOA 2015 7

In 2014 – During Every Minute, of Every Day, We:

- **Sent 204M e-mails**
- **Shared 684K posts on Facebook**
- **Posted 36K pictures on Instagram**
- **Sent 100k tweets on Twitter**

The more data you share, and the more ways that you share, or interact on-line, the easier it becomes to create a digital fingerprint used to establish your pattern of life –
who you know and where you go, what you do and who you're doing it with, where you shop, and also where you are right now locationally and where you are likely to be in the future.

Marketers and data brokers know this, and determined criminals can know it too.

Oh, Do We Share

- You Are The Product
- Terms of "Service"
- Misplaced Expectations

NESTOA 2015 8

Almost everything is for sale on the Internet – but most especially YOU:

And you don't own the data you post, you don't own your mobile or other gaming results, and you don't own your search results, – not on Facebook, not on Angry Birds and especially not on Google, which saves and stores every search you've ever made.

This is established in the "Terms of Service" in the many applications that you use, which of course no one ever actually reads – on average each year we see more than 1400 of these terms having an average of 2500 lines each, that would take us 76 eight-hour working days to plow through.

So your data is out there and is available to be sold and used by anyone that can pay for it. Or steal it..

In its defense in a recent lawsuit, Google actually made the claim that "a person has no legitimate expectation of privacy in information he or she voluntarily turns over to 3rd parties"- so if you email a Gmail user, by their argument you have automatically waived any privacy rights and consented to the sale of your message's contents. This would be true even though you don't have a Gmail account yourself.

Mobile operating systems are simply a new frontier for the collection and use of information by others about you.

We expect that by appropriately using our "'Profile Settings" that we can limit the amount of sharing that we do. But that expectation is misplaced.

Identity Theft

Children are 50 times more likely to be the victims of ID theft (500k annually)
- Carnegie Mellon University's CyLab

NESTOA 2015 9

It's estimated that 90% of all U.S. children aged 10 to 23 have at least one social media account.

The other especially vulnerable demographic is the elderly – ironically, while the criminals are doing business on-line, the elderly are much less likely to bank on-line and use e-mail, and so do not check their accounts frequently and fail to discover when questionable activity occurs.

Identity Theft

Social media accounts compromised:

- LinkedIn
- Twitter
- Yahoo
- Snapchat
- Google
- Facebook

NESTOA 2015 10

Security engineers at FB have acknowledged that 600,000 Facebook accts are compromised – every day.

That's only the beginning:

- 55% of on-line customers use same PW for multiple websites
- 30% of us use same log-in
- 40% don't use a security code to lock and unlock access to our phones

– so very likely after a compromise, your other accounts and data are also targeted.

It is likely that the majority of these <u>social site</u> breaches are committed by transnational organized crime groups.

Identity Theft

Where does our data go?

- Spokeo
- Reed Elsevier
- Acxiom
- Experian
- Datalogix

NESTOA 2015 11

Where does all of this data we share go?

Vast terabytes of it is gathered by Data Brokers:

Spokeo
RELX
Acxiom
Experian
Datalogix

These companies and others –are part of a $156 Billion Dollar industry.

What is their record regarding protecting data?

Identity Theft

Documented Hacks and Breaches of Data Brokers

- Experian
- Acxiom
- LexisNexis
- Dun & Bradstreet

NESTOA 2015 12

Not so great. Beyond the Choicepoint breach, which some of you may remember from a few years ago:

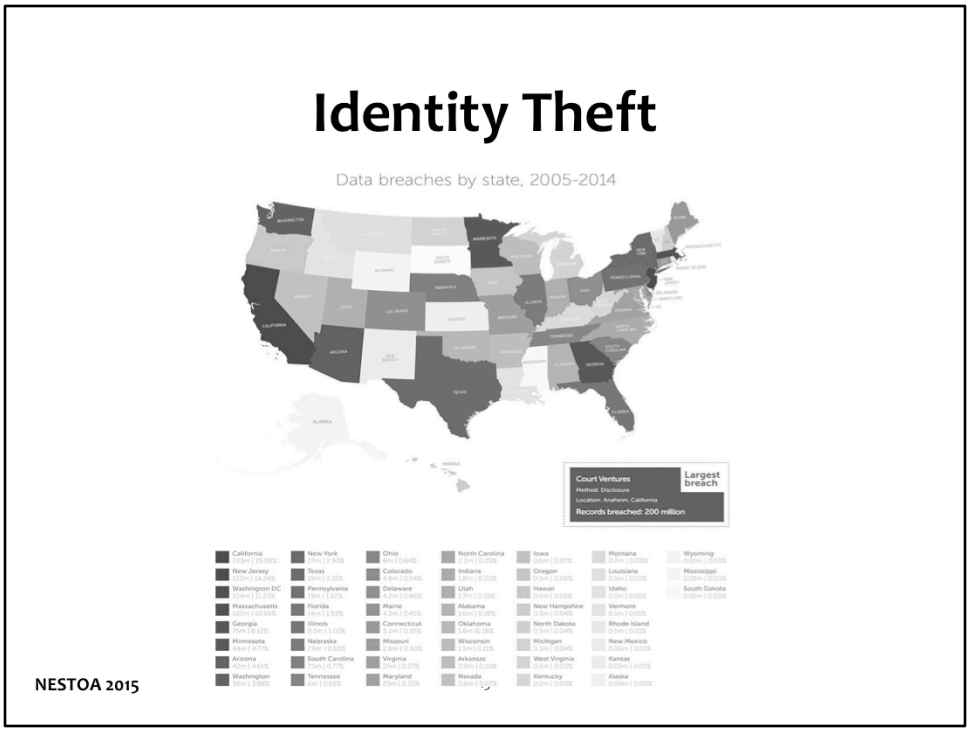
In the Experian event:
- **Russian hackers attacked AnnualCredit Report.com and**
- **Posted celebrities' and politicos' complete credit reports**
  – those for Michelle Obama, Joe Biden, Lady Gaga, Beyonce, Bill Gates, and others

The Data Broker Axciom is in possession of data representing 96% of American households with:

- **- 20 billion records on file**
- **- covering some 300 million individuals**
- **- processing 1.5 billion records per day**
- **- with 1500 data points in each record**
- **- and used for behavioral or predictive targeting**

They've suffered two separate breaches of data, although thankfully, not recently.

BTW - No federal statute provides consumers with the right to learn what information data brokers have compiled about them, although a few states have such laws.



Here's a map of data breaches - by state – from 2005 through 2014.

You won't be able to read the Key -

But just in each of the darkest shaded states?

Experienced compromised records of 6 or more million. The total is 930 Million over the decade.

Identity Theft

<u>Dark Web Content</u>

- Pirated goods
- Drugs
- Counterfeit currency
- Cards/accounts
- ID Theft
- Child abuse images
- Fake personal documents
- Weapons
- Human and organ trafficking

NESTOA 2015 14

There is boundless illicit activity on the Dark Web - ID theft and compromised financial information do not even account for most of the volume

– which by the way is estimated to be 10 times the size of the Web that you and I use every day.

Identity Theft

- GRAMS – a "Google" for the Dark Web
- Russian Business Network (RBN)
- ShadowCrew
- Profiling

NESTOA 2015 15

There is actually a a "Google" for the Dark Web - you can search for the criminal activity of your choice and comparison shop; malefactors can actually pay to have their results listed first by buying keyword search terms.

The Russian Business Network is a multi-product line, full-service cyber-crime organization – and is used by many of the world's most prolific e-mail spammers– those emails that invite you to click on a link to purchase pharmaceuticals or help African princes free their fortune.

The ShadowCrew is reportedly responsible for stealing and selling 180 M credit & ATM cards.

And we are seeing the growth of profiling - some unscrupulous data brokers may be catering to criminals, creating data profiles on individuals ready-made for crime, much as legitimate data brokers create them for on and off-line businesses.

Identity Theft

Sale of "Fullz"

- Name
- Address
- SSN
- DOB
- Workplace addresses
- Bank account & Routing #s
- State DL #
- Mother's maiden name
- E-mail address
- Other-account Login/PWs

NESTOA 2015 16

What can you buy, Identity-wise?

"Fullz" (more complete identity records, as you see here) are among the most prized identity data.

These ID theft records can contain the elements listed – and more.

By the way, fake State Driver's Licenses (for any state) can ship from Russia or China for about $200.

Identity Theft

Rising: Health Care ID Theft

- Community Health Services
- 206 hospitals in 29 states
- 4.5M records
- Social Security numbers and other personal data

NESTOA 2015 17

The CyberSecurity provider Mandiant has recently seen a spike in cyber attacks on healthcare providers:

The information stolen from Community Health included:

- **patient names,**
- **addresses,**
- **birth dates,**
- **telephone numbers,**
- **and the Social Security numbers**

of people who were referred or received services from doctors affiliated with the hospital group over the last five years.

This event of course was eclipsed, in tsunami-fashion, by the Anthem Health Care breach.

Identity Theft

Professionalization of CyberCrime is Here

- Automated systems and scalable architecture
- Untraceable payments (Bitcoin and other forms of crypto-currency)
- Consulting services and training
- Customer help desks
- Criminal gang PII data warehouses

NESTOA 2015 18

So the professionalization of CyberCrime is with us, and features:

- **Automated systems & scalable architecture**
- **Untraceable payments (using Bitcoin and other forms of crypto-currency)**
- **Consulting services and training (including "how-to" videos, YouTube style)**
- **Customer help desks**
- **Criminal gang data warehouses of Personally Identifiable Information**

So what are we left with?

– Criminals are now in the knowledge management business.

And new technologies roll on and the reach of the Web continues to expand –

In the mobile arena:

Radio Frequency ID technology - Hacked
Near Field Communications (used in Apple Pay, for example) - Hacked
Bluetooth - Hacked
The Samsung, HTC, & Apple Unique Fingerprint ID – all Hacked

The mobile problem is bad and getting worse – phone Operating Systems and Apps can be very insecure.

So insecure, and the tools to enable compromise so cheap and available, that domestic violence shelters have learned to take away a new client's phone, remove the battery and dis-assemble it to eliminate the possibility of tracking the client.

The new iPhone 6, available last week (anyone have one yet?), is said to have an unmatched screen resolution:

- **Enabling Millenials to take those ubiquitous selfies they've become fond of …**
- **possibly meaning that theft of that particular identity biometric will perhaps become simpler in the future.**

Identity Theft

Internet of Things
- Billions more devices connected to the Web

- Products we use every day
- Automobile processor content in 2015
- Most Hackable?

- Google's self-driving cars
- Expect same ToS

NESTOA 2015 20

And then there's the Internet of Things - -> soon, billions more devices connected to the Web.

But the products that we use every day –

interior and exterior lights, home security systems, coffeemakers, door locks, thermostats, blood glucose monitors, babycams – all have been Hacked.

Processor content in automobiles is ever-increasing – it's now said that a car is a Computer on Wheels

- **The Average vehicle contains 70 to 100 Electronic Control Units, and100 M lines of computer code**

Most Hackable? (according to security researchers):

- **Jeep Cherokee, Cadillac Escalade, Infiniti Q50, Toyota Prius**

- **Google's self-driving cars – Hacked**

And we can expect those same Terms of Service – all data will be available to others for collection and use, and so also available to criminals.

If we believe that better, newer technology is the answer to our fraud issues, perhaps we should consider again.

Identity Theft

New Frontier: The Cloud

- 1980: 1 Gig storage/month = $437,000.00
  Today: → $0.026
- Cloud Cracker

NESTOA 2015 21

The New Frontier is The Cloud:

Beyond the many other imperatives impelling its use, simply from a storage cost perspective, economics mandate movement of our systems to the cloud -

In 1980: 1 Gig storage/month = $437,000.00
Today: → $0.026

But the Power of the Cloud is available to us and to bad guys alike:

Cloud Cracker was software used in the rental of the power of Amazon cloud servers by criminals, to break encryption algorithms and was used in the recent Sony PlayStation hacks.

So the cloud itself can be a tool in the hands of the bad guys.

NOTE: Much of the material covered in this first half of the presentation is sourced from Future Crimes (©2015) by Marc Goodman, an invaluable resource for understanding the threats that exist in the on-line environment. He is the founder of the Future Crimes Institute. You can see http://www.futurecrimes.com/about/mg/ for more.

FTA Fraud Efforts

Identity Theft Driven Tax Refund Fraud

Joint Countermeasures

NESTOA 2015 22

So the Risk Matrix or Harm Probability Categories out there are pretty ubiquitous … but more pertinent to our work, what is the effect of fraud on our tax filing environment?

Simply, beyond the very significant fiscal impact, the continued problem of identity theft-driven fraudulent tax refunds erodes confidence in the tax system and increases burden on those taxpayers who comply with the tax laws.

So let's talk about our own efforts to address it over the last 10 months.

But as a preface, you have by now heard about and possibly seen documents describing new anti-fraud measures for the upcoming filing season.

These measures are the product of a small group of representatives of the states, IRS, and industry - and not by all states, it's true.

But I think the term exigency, defined as a situation requiring swift action to prevent harm, applied here.

We needed to act with all due and deliberate speed to ensure a useful response to fraudsters during the 2016 filing season. And we believed we had a good mix of folks to consider the measures under consideration.

FTA Fraud Efforts

"The perfect is the enemy of the good"

NESTOA 2015 23

So an historical reference, since here in Mystic, and we're in one of the original 13 Colonies:

Our Declaration of Independence was not created by the Continental Congress, but by an appointed committee of five. Even in this little number, there were strong opinions represented.

Although the committee included John Adams, a firebrand who was fiercely desirous of extending to the utmost the privileges and rights of the colonials, he selected Thomas Jefferson to be its scribe, as Adams knew that if he wrote it, it was likely to be controversial.

In this way and with intense discussion by the group, the document came to be a reasoned and practical expression of the common will.

That is what we have tried our best to accomplish in these very initial steps to create fraud measures.

Still and all, the Declaration, and the subsequent United States Constitution, were not complete works; the rights and privileges they secure for all of us have been improved upon over time.

So it will be with our fraud work. And the many states, companies, and the IRS will all be needed to continue this effort. So we will look to all of you to do your part to assist.

FTA Fraud Efforts

FTA Suspicious Filer Exchange

- Enables states to share information on refund fraud schemes through regularly scheduled monthly conferences calls and data transmission via encrypted software
- Program became more active in late 90's and now has 40+ participants.
- IRS joined calls in early 2014

NESTOA 2015 24

FTA and the states have been involved in this area for a long time, in large part via regular communications among the states on fraud.

The Suspicious Filer Exchange grew thru the 90s and now has more than 40 participants, including the IRS.

Work is needed to improve this process to include the full participation of all state members. Not all members share their fraud findings – some only receive – and others only share with a limited number of other states.

That has to change if we're going to do the most effective job we can, together.

FTA Fraud Efforts

FTA-NACTP Fraud Working Group

- Joint effort by states, tax software industry and IRS to improve fraud detection and prevention
- Principal focus – establish a trusted customer standard from both the industry and the state perspective
- Program began October, 2014

NESTOA 2015 25

Also, recognizing that action was needed to engage industry in this activity with us, almost a year ago FTA also created a state-industry group to address fraud, with the National Association of Computerized Tax Processors, a body that we've worked with on standards for over 20 years.

Many of our group's aims and work items were later adopted as a part of the IRS Summit process -

In particular some of the added e-file submission data elements designed for use in the State Trusted customer analysis, and the aim and structure of the Industry Trusted Customer requirements.

FTA Fraud Efforts

States-IRS Fraud Data Exchange

- Pilot program between IRS and four states in which returns determined by IRS to be fraudulent or suspicious are shared with states
- Information shared was all fraudulent returns from 2014 filing season and suspicious return information from 2015 filing season
- Program began in November, 2014
- Target – all states receiving data before 2016 filing season

NESTOA 2015 26

IRS joining the Suspicious Filers Exchange last year paved the way early this year for the Service to propose a new State-IRS exchange in which IRS would share returns determined to be - or suspected of being - fraudulent.

Here our pilot states' experience showed that after analysis, the states found fraud not previously uncovered at the state level, and likewise the state determined that there was refund fraud present in situations where the IRS had not.

So this program needs to be expanded as soon as feasible to all states, and that is what IRS intends.

FTA Fraud Efforts

<u>Work with Financial Institutions</u>

- An effort involving states, banks and NACHA to facilitate the return of refund monies to states by financial institutions via Leads and Opt-ins
- IRS has had programs in place since 2012 and 2014
- Ohio and Michigan began similar programs in 2014 and 2015
- Can be used as models for other states

NESTOA 2015 27

FTA also reached out to the financial industry, to learn about what can be done in the area of refund recovery – monies that banks suspect or know represent fraudulent refunds that could be returned to the state.

There are two aspects to this – Leads that banks can report to the state for agency investigative action and request that the funds be returned, and rules for an opt-in program where banks can stop and then return funds via the banking system where the presence of fraud is certain.

IRS has recovered 5 Billion dollars via these steps since 2012.

At least four other states, in addition to OH and MI, are working on starting their own programs, and we expect their efforts in that direction will be aided by the work of the new Summit Financial Products group.

IRS-States-Industry Summit

IRS-States-Industry Fraud Summit

- March 19, 2015 – IRS Commissioner convened an unprecedented Security Summit meeting in Washington, D.C.

NESTOA 2015 28

Following the emergence of significant problems early in this filing season, the IRS Commissioner convened a Summit on Identity Theft Refund Fraud in Washington.

Participants were IRS and Treasury officials, state tax administrators, and CEOs of leading tax preparation firms, software developers, payroll and financial products processors.

We agreed to come together in a partnership committed to protecting taxpayers and the tax system.

IRS-States-Industry Summit

Three working groups:

<u>Authentication</u>

- To establish procedures for strengthening authentication practices, including new ways to validate taxpayers

NESTOA 2015 29

Doreen Warren of Idaho is our overall coordinator of the state participation in the Summit fraud effort.

Doreen is also Chair of our FTA-NACTP Fraud Working group and was a key contributor to the creation of the industry and state trusted customer measures.

The Authentication group was charged with developing methods for enabling industry to better ID proof taxpayers and provide additional data in the actual taxpayer filing submission, to permit states and IRS to have greater confidence that a filed return was in fact generated by the taxpayer.

"Trusted customer" standards were built for industry to use in creating a taxpayer account and validating an existing account, including:

- **- standards for password use and security questions,**
- **- the use of out-of band text or e-mail taxpayer confirmations,**
- **- as well as queries to make of vendors during the vendor approval process as to their practices.**

For government use, 29 new return data elements were identified for submission with the tax return. Best practices are being developed for states to be guided by in the use of the new data elements.

The use of these during 2016 will be monitored - and reported on - as to their effectiveness, in order to alter and improve the measures for 2017.

IRS-States-Industry Summit

Information Sharing

- To find opportunities for sharing information to improve the participants' collective capabilities for detecting and preventing fraud

NESTOA 2015 30

The Information Sharing is group focused on creating an ability for industry to securely report to the states and IRS aggregated and anonymized data relating to patterns in the returns that they see that indicate fraud.

The target date for release of the details of the formats of these reports is October 30, so that programming may begin.

The other needed activity was the creation of authority for the states and IRS to require industry reporting; FTA created language for states to employ in their vendor operating agreements for this purpose.

In addition, this group is now developing a method for IRS and the states to share with industry aggregated results of their fraud analysis to assist tax provider companies in improving their own fraud checks.

IRS-States-Industry Summit

Strategic Threat Assessment and Response

- To focus on business model technical issues and measures aimed at best practices in protecting data and preventing fraud

NESTOA 2015 31

The Strategic Threat Assessment and Response group, populated by Technology Officers and Information Security Officers, will more generally focus on:

- **- business model technical issues and measures**
- **- aimed at best practices in protecting data and preventing fraud,**
- **- using the National Institute of Standards and Technology risk model**

Working together should enable better allocation of security resources to emerging threats, including identifying the right problem and addressing it with the right solution.

IRS-States-Industry Summit

IRS Commissioner Announcement

- **June 11, 2015 – An agreement in the form of a Memorandum of Understanding was announced which reflected the efforts of the participants**

NESTOA 2015 32

On June 11, 2015 – An agreement in the form of an MOU was announced which reflected the efforts of the participants.

Specifically, the MOU recommended that Summit participants:

- support the measures under development to validate returns from trusted customers

- establish a minimum set of standards that Industry must use in analyzing and reporting indicators of potential fraud, and

- research the creation of an Information Sharing and Analysis Center (ISAC) to facilitate real-time information sharing

All of these efforts are underway, and at this point I believe that 30 states have signed the MOU, and more to come, which simply communicates an endorsement of the cooperative working process that the Summit is meant to facilitate.

IRS-States-Industry Summit

July 2015 - Four additional groups subsequently formed:

- Taxpayer Messaging
- Financial Products
- Information Sharing and Analysis Center
- Professional Products

NESTOA 2015 33

Moving forward, four additional working groups were formed:

Taxpayer Messaging - Will focus on developing consistent taxpayer communications regarding identity theft refund fraud and actions taken by the IRS, states and industry.

Financial Products - Will work with financial institutions and others including the Financial Services Roundtable, a group of larger banks, and the National Prepaid Debit Card Association, to examine and address fraud and refund recovery issues.

Information Sharing and Analysis Center - Will develop a method for the IRS, states and industry to more rapidly share information, including early warning detection of emerging threats.

BTW ISAC bodies are now found in many situations where public sector organizations need to facilitate communications with the private sector:

- Aviation, Financial Services, Oil and Gas, Information Technology, CyberSecurity, at the state government level, and many others

Just a note - The automobile industry recently created an ISAC to address the issues involved in its products, which as we've seen not only have a high "information content", but which now and in the future will be constantly connected to the Internet.

And Professional Products – Intended to focus on non-DIY situations where the customer is often present, and measures to improve detection and prevention of fraud in that environment.

This last group is forming now. If your agency has an interest in participating in it, please contact

The Future

Immediate Issue:

Industry Compliance: Know Your Customer

NESTOA 2015 34

The new requirements on the tax software industry regarding Know Your Customer are substantial – and are critically needed.

Finalization of them also came at a time when development on products for 2016 was largely already complete.

In order to reduce burden on industry and the states, a committee of IRS and State personnel has been created that will receive e-file vendor submissions describing their approach to compliance with the Industry Trusted Customer requirements and vet them, making a determination in the nature of a provisional approval.

This will save the companies from having to go through the process 42 times, and assist states (especially those with limited staff) from additional review burden.

However the decision on each vendor will then be communicated to all states, which of course have ultimate authority regarding whether the vendor is approved.

Going forward we expect to use our website, now undergoing significant revisions, to create the needed communications infrastructure for this activity.

The Future

Governments and Markets Are Moving:

- In a recent survey with 235 financial provider respondents from across the world, biometric services are a priority:
- 22% of banks already offer biometrics to their customers
- 65% are planning to offer such services in the near future
- More than half plan to launch fingerprint biometrics for their end users
- An additional 21% are focusing on voice recognition

NESTOA 2015 35

What does the Future Hold?
Financial providers realize that the game is changing regarding Customer Identification Protocols.

So, many are looking to Biometrics.

This represents a move away from Knowledge-Based Authentication – things the customer knows.

As we've seen, there may be issues with the use of biometrics in the future, as they involve markers which ostensibly can't be changed, and thus may represent a greater threat to the maleficent acquisition of one's identity with their use.

You'll also note that Knowledge-Based Authentication is what our tax agencies and companies will be relying on, in part, for the next filing season.

As we well understand, we are catching up to the broader market in the use of these steps, and so recognize that we have to continue to improve the ID proofing measures that we implement.

The Future

Governments and Markets Are Moving:
From FTA's TaxExpress:

- **[The U.S.] Treasury will use an anti-money-laundering tool for the first time to combat stolen identity refund fraud in South Florida.**

NESTOA 2015 36

A geographic targeting order, recently issued by Treasury's Financial Crimes Enforcement Network, will require Florida check cashers in Miami-Dade and Broward counties to gather additional information from people attempting to cash tax refund checks over $1,000, including:

a copy of the customer's identification,

a digital photograph of the customer taken at the time of the transaction,

the customer's phone number

and the customer's thumbprint.

Their experience should be enlightening.

The Future

Governments and Markets Are Moving:

- **State use of identity confirmation outreach to taxpayers**
- **Will continue to be necessary**

NESTOA 2015 37

Also, many states this filing season were put in the uncomfortable position of using of identity confirmation outreach to taxpayers.

However - the states' experience from this filing season was that taxpayers have proven to be quite willing to undergo additional checks on their identity, complete surveys, and respond to questions, and the like - if they perceive that the agency is engaged in the activity to protect their identity.

So although it's regrettable that such measures are necessary, we do have an understanding and cooperative citizenry.

These steps will no doubt continue to be necessary.

The Future

What Can I Do?

- Appropriately resource fraud unit
- Engage emerging Summit recommendations
- Adopt industry and state authentication standards
- Prepare to use the industry leads data and to provide feedback to them
- Investigate financial process improvements

NESTOA 2015 38

What Can I Do? Some Suggestions:

Resource your fraud unit
Perhaps it should be multi-disciplinary and coordinative, with responsibilities centered and not spread across the agency

Make the the best use of the Suspicious Filer Exchange and also the IRS data that will be forthcoming

Engage the finalized and emerging Summit Recommendations - And monitor the effectiveness of the steps you take

Adopt the industry and state authentication standards for 2016
Use the trusted customer procedures and requirements and be guided by "lessons learned", and contribute your feedback on their effectiveness

Prepare to use the industry leads data and to provide feedback to industry
We expect that the data types and formats for that reporting will be compete by October's end.

Develop and implement financial process improvements
We need new measures in this area and consistency across states
Including:

- better identification of outgoing tax refunds
- and agency exploration of a financial institution opt-in program for refund recovery

The Future

Continued Effort and Cooperation

- FTA Teleconferences Planned:
  - Weekly
  - Mid-October-early December and continuing
  - Updates on Summit group work
  - Best practices, use of data, communications, Q&A

NESTOA 2015 39

We plan to begin a series of sharing teleconferences for states to keep agencies updated on the work going forward, and to provide an opportunity to share information on:

- best practices,
- communications strategies,
- use of the new data, and
- the need for additional common actions, and
- reviewing the status of the Summit work along with Q&A sessions.

I believe we've set Wednesdays at 3:30 Eastern Time for those calls.

The Future

- FTA and State Action
- IRS Facilitation
- Industry Cooperation

NESTOA 2015 40

Regarding uniformity:

FTA has a 25 year history and track record of bringing disparate viewpoints together – industry and state, and IRS when needed – to achieve consensus in numerous areas of electronic tax administration as well as other areas – many of you know our record on this.

We need to remember that it is better to achieve accord among nearly all states, than to provide no collaboration, no leadership, no drive to consensus at all, and have accord among none.

So although we can't pledge that all states will adopt every one of the Summit measures devised, we can say that if we work effectively together on these measures, the potential for disparate requirements will be greatly lessened, and our effectiveness in addressing the problems we face will be greatly enhanced.

For IRS's part, it has stepped up and contributed significant resources to provide an organizing force that will help all parties focus on workable solutions and assist all of us in doing a better job of fraud detection and prevention.

And Industry has been ready with thoughtful input thus far on the measures proposed to ensure that the activities undertaken in this effort truly help the states, the IRS, and the taxpayers.

Fraud Identification and Prevention

Questions

Jonathan Lyon
Sr. Mgr., Tax Technology and Standards, FTA
Jonathan.Lyon@taxadmin.org

NESTOA 2015 41

We know that all of the things that we have addressed in our work to date to combat tax fraud are not done, will never be done, and the contributions of many others will be needed going forward to ensure that our actions effectively target the on-line malefactors who prey upon our taxpayers.

All of us must do all we can to assist, in our own states and by contributing our expertise to this joint effort.

The very serious problems we are having with fraud brings us a new tax filing world – and providers have to be prepared to sell something somewhat different than in the past:

- → **of course, simplicity and convenience and accuracy, but in addition,**
- → **security of the taxpayer's Personal Data**
- → **and not necessarily a fast tax refund.**

All of us must do this together, so that taxpayers are protected and do not lose confidence in their providers and in government when filing electronically.

Again, for a discussion of the threat environment we face, the recently published Future Crimes (© 2015 by Marc Goodman) is highly recommended.

Thank you for affording me an opportunity to talk with you.

- **If we have time for questions I'd be happy to take them.**

Fraud Identification and Prevention

Questions

Jonathan Lyon
Sr. Mgr., Tax Technology and Standards, FTA
Jonathan.Lyon@taxadmin.org

Postscript: What You Can Do:

Use a security code for your smartphone
Use longer passwords not likely to be guessed and a password manager
Careful in your use of Public Wi-Fi
Surf safely
Be smart with use of social media
Keep your e-mail secure
And - perhaps - answer those security questions incorrectly, or use a semi-random string