IRS's CP-2000 E-Mail Scams - Never in Dubai - Common in Canada & the UK

Richard Thompson Ainsworth

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship

Part of the Banking and Finance Law Commons, International Trade Law Commons, Science and Technology Law Commons, and the Tax Law Commons
IRS’S CP-2000 E-MAIL SCAMS – NEVER IN DUBAI – COMMON IN CANADA & THE UK

Boston University School of Law
Law & Economics Working Paper No. 17-07

Richard T. Ainsworth
Boston University School of Law

This paper can be downloaded without charge at:

http://www.bu.edu/law/faculty-scholarship/working-paper-series/
IRS’S CP-2000 E-MAIL SCAMS – NEVER IN DUBAI – COMMON IN CANADA & THE UK

Richard T. Ainsworth

On September 22, 2016 the Internal Revenue Service (IRS) and its Security Summit partners issued an alert to taxpayers and tax professionals to be on guard against fake e-mails purporting to contain a tax bill related to the Affordable Care Act. Surprisingly, this e-mail scam works. It really should not.

Modern technology is facilitating many contemporary tax scams. In recent years the US has seen false (refund) return scams, phone scammers impersonation IRS agents, and now e-mail scams with fraudulent CP-2000 notices attached to a demand for payment. The same phone and e-mail frauds have appeared in both Canada and the UK. The timing of the Canadian and UK frauds suggest a migration of the phone fraud.

3 The pattern of frauds in the UK, and moving to phone scams with the idea of using phone scams and iTunes cards apparently coming from the US. Half million pound iTunes Gift Card Scams, GET SAFE ONLINE (August 11, 2016) available at: https://www.getsafeonline.org/news/half-million-pound-itunes-gift-card-scams/ (indicating that the fraud in the UK exceeds £520,000, and that one individual lost £46,000 to the scammers posing as HMRC employees). Steven Chisolm, Fresh Warning Issues over iTunes Gift Card Scam, THE NEWS (August 8, 2016) available at: http://www.portsmouth.co.uk/news/crime/fresh-warning-issued-over-itunes-gift-card-scam-1-7516308 (indicating that the iTunes card variant of the HMRC impersonation fraud first appeared in the UK in May 2016); iTunes Gift Card Scam Spreads to UK, PENTLANDS LTD. (ACCOUNTANTS) available at: http://www.pentlands.ltd.uk/resource/itunes-gift-card-scam-spreads-uk (indicating that the UK believes that the phone scams spread from the US into the UK); Callum Brodie, WARNING! Now it’s not just Scam HMRC emails – expect calls too, MSEN (June 30, 2016) available at: http://www.monesavingexpert.com/news/phones/2016/06/warning-fake-hmrc-calls-on-the-rise---what-to-
from the US to the UK and Canada. That is the analysis of the UK’s Action Fraud Agency, part of the National Fraud Intelligence Bureau (NFIB) within the City of London Police Department.4

From a US perspective, the timing of the UK and Canadian migration appears right on target with the Action Fraud assessment. The arrest of a US phone scam “ringleader,” Sahil Patel, on December 18, 2013 seems to have set the migration in motion.

However, the conviction and sentencing of Sahil Patel to 14 years imprisonment on July 8, 2015 apparently had a different effect in the US. Here we have seen the mutation of this fraud into the present e-mail scam.5 By late October 2016 the US was indicating in court documents that our phone scam was probably not a home-grown fraud. The US fraud was not thought-up by Sahil Patel. He was a foot soldier, The US phone scam was planned and “… organized by conspirators in India.”6 It is probably not a coincidence that as the US closed in on this fraud, the very same fraud began to accelerate in the UK and Canada.

The Indian government has begun an enforcement action against a number of call centers outside Mumbai related to the IRS impersonation phone scam. Allegedly an “… informer went to the [Indian] authorities a few weeks ago.”7 This report suggests that the Indian enforcement action was independent of the US, UK or Canadian investigations. The Indian arrests were for offenses committed in India, but where the losses were

---

4 do-if-youve-been-targeted (indicating the migration of e-mail based frauds to telephone scams searching for PII or taxes alleged to be due); Simon Wells, Warning: Can you Really Trust that call from HMRC is Genuine? QTAC PAYROLL (September 2016) available at: http://www.qtac.co.uk/qblog/2016/07/warning-can-you-really-trust-that-call-from-hmrc-is-genuine/ (indicating that some scams allege that the victim’s PAYE has an overpayment to secure PII, or that additional taxes are due); HMRC, Avoid and Report Internet Scams and Phishing, GOV.UK available at: https://www.gov.uk/report-suspicious-emails-websites-phishing (explain how to respond to suspicious calls and e-mails); Scam Warning: Phone Message Threatens HMRC Lawsuit, TAX HELP FOR OLDER PEOPLE, available at: http://www.taxvol.org.uk/scam-warning-phone-message-threatens-hmrc-lawsuit/ (indicating that elderly people are a target group for this scam in the UK); Sean Keach, iTunes Gift Card Scam Revealed – one victim paid out £15,000, TRUSTED REVIEWS, available at: http://www.trustedreviews.com/news/apple-itunes-gift-card-scam-revealed


7 US Attorney, Southern District of Texas, Dozens of Individuals Indicted in Multimillion-Dollar Indian Call Center Scam Targeting U.S. Victims, (October 27, 2016) available at: https://www.justice.gov/usaosdtx/pr/dozens-individuals-indicted-multimillion-dollar-indian-call-center-scam-targeting-us. US v. HGlobal is the result of a multi-agency, three-year investigation into the phone scams that brought 61 individuals and entities to court on criminal conspiracy, wire fraud and money laundering charges. This case is going to trial in the Southern District of Texas, Houston Division and involves 20 individuals arrested in the US, 32 others in India along with 5 Indian call centers.

realized overseas. Extraditions are likely.8 “[Indian] authorities arrested 70 people Wednesday [October 5] alleging that they helped manage nine call centers where about 700 people made thousands of calls a day to try to trick Americans into sending money.”9

If past patterns prevail one might expect that closing the five call centers identified in the HGlobal indictment10 would only mean that other call centers would take up the business, and the fraud would continue. The same frauds, from the same Indian call centers also appear to be behind a phone fraud up-tick in Australia,11 and New Zealand.12 Following the same pattern, Irish phone frauds recently morphed into e-mail scams purportedly coming from Irish Revenue, which the Irish believe migrated into Ireland from the UK.13

This is like a game of “whack-a-mole.” When a tax scam gets put down in one area we tend to see both:

(a) a migration of the fraud to other jurisdictions (the US phone scam’s migration to Canada and the UK), and

(b) a domestic mutation of the fraud (the US phone scam morph into the CP-2000 e-mail scam.)

New scams pop up whenever old scams are put down.

There are lessons to be learned. Not only is international cooperation essential when frauds are foreign inspired, fast moving and technology based, but heightened attention needs to be paid to structural weaknesses in the domestic tax codes, processes, and procedures, because mutating tax scams seek out and take advantage of weaknesses wherever they exist.

---

8 32 of the 61 defendants in the HGlobal case are listed as Indian nationals.
10 The call centers identified were: HGlobal; Call Mantra (d.b.a. Robust Inc., Raytheon International; Worldwide Solution; Zorion Communications PVT. LTD.; and Sharma BPO Services.
In their hay-day, the *false return scams* in the US generated at least $500 million in “profit.”\(^{14}\) Until recently, the US phone and e-mail scams never appeared capable of reaching these levels of “profitability.” As recently as October 1, 2016, the Wall Street Journal was reporting that collectively the phone and e-mail scams stole roughly $47 million from more than 8,800 individuals.\(^{15}\) However, the unsealed Houston indictment indicates that the numbers are much higher. For just the *phone scam* alone $300 million was scammed from over 15,000 individuals between 2012 and 2015.\(^{16}\)

This paper focuses on the new *e-mail scams*, a mutation of frightening potential. It is a technology-based scam, and it has the capability to eclipse all the older scams. It needs to be taken very seriously. The problem in both the phone and e-mail scams is very simple – how can a taxpayer quickly and easily confirm the accuracy of an assertion of tax liability posed in an e-mail, letter or phone call when the matter is presented with an urgency that does not leave a lot of time for consultation and consideration?

A solution is available. Government technology in the UAE would prevent it. Dubai would help its citizens identify and block this scam with confidence, in much the same manner as the IRS plans to use “verification codes” to block false W-2s.\(^{17}\) This paper proposes a Dubai type of solution to the current *e-mail scam*. The US, UK, Canada, Australia, NZ, and Ireland should do for its citizens what Dubai does for theirs – adopt a technology solution. The cost is an infinitesimal fraction of the losses.

**HOW DID THE E-MAIL SCAM ARISE?**

In the current *email scam* taxpayers receive an e-mail attachment (allegedly a bill from the IRS) that is a reasonably good reproduction of IRS Notice CP-2000.\(^{18}\) A true

---


For Processing Year 2011 (through September 10, 2011), the IRS reported that it had identified over 1.6 million tax returns with more than $12 million claimed in fraudulent tax refunds … [and] of the 1.6 million tax returns identified as fraudulent for Processing Year 2011, a total of 851,602 of these tax returns, with $5.8 billion in associated fraudulent refunds, involved identity theft. … [But,] overall, the IRS does not know how many identity thieves are filing fraudulent returns and how much revenue is being lost.

The testimony indicates (at 7) that the IRS claims to have prevented 94% of refund frauds or $11.5 billion, which leaves $500 million unaccounted for.

\(^{15}\) Laura Saunders, *The New IRS E-mail Scam*, WSJ (October 1, 2016) at B7.


\(^{17}\) This effort was part of the IRS’s real time initiative. IRS News Release, IRS to Host Second Real-Time Tax System Meeting, IR-2012-10 (January 18, 2012), Tax Analysts Doc 2012-963; *IRS Tests W-2 Verification Code for Filing Season 2016*, available at: https://www.irs.gov/individuals/w-2-verification-code.


CP-2000 is a computer generated notice from an IRS data-matching program (the Automated Underreporting Program) which identifies variances between return information provided by the taxpayer and information reported to the IRS by third party employers, banks and businesses on Forms W-2, 1090 and 1099.

A true CP-2000 is not a bill. It is a notice from the IRS that there is an apparent mismatch in IRS data. It is not a demand for payment nor is it an audit determination. The CP-2000 simply asks a taxpayer if they can explain a variance. But, that’s not how the fraudsters are using it. In the hands of the scammers a fake CP-2000 becomes a demand note for immediate payment.

The e-mail scam is developing in response to the three-year IRS phone scam enforcement action that culminated in the HGlobal grand jury indictment unsealed at the end of October 2016 in the Houston District Court. Two of the four “domestic managers” of the phone scam, who reported to Sahil Patel, live in the Houston area. Is it just a coincidence that 160 miles to the west of the Houston courthouse is the Austin post office box where the national CP-2000 e-mail scam demands that taxpayers remit their payments?

In the March 2015 Report to Congress the Treasury Inspector General for Tax Administration (TIGTA) summarized the phone scam. He stated that fraudsters making calls would deal with skepticism on the part of taxpayers with declarations of authority. For example callers would “… use a fake name, tell[ing] the victim a made-up badge number, and claim[ing] that the victim owe[d] taxes and [was] criminally liable for the amount owed…. [callers presented evidence of authority by reciting] the last four digits of the victim’s SSN …”

The phone scam brought in hundreds of millions of dollars, but it suffered from a lack of plausible evidence that the caller was indeed an IRS agent. At some point an enterprising fraudster hit upon the idea of producing fake CP-2000s to buttress assertions of liability. In March 2016 TIGTA reported that, “… individuals claim[ing] to be IRS employees on the telephone [were] misus[ing] IRS logos, seals, or symbols to create official-looking letters and e-mails.”

(posting a copy of a fake CP-2000 notice marked up by the authors to show where the variances are with a true CP-2000, and observing:

I was surprised when we got our hands on one of the fake letters; it looks pretty legit. I also thought it was smart of the scammers to only ask for $325.00 … a reasonable amount. And if someone took the time to call the IRS to see if they owed this money, there’s a good possibility they would be put on hold for 2 hours before getting a “courtesy disconnect” due to the long hold times.)

19 The four domestic managers are Sunny Joshi and Rajesh Bhatt (a.k.a. Manoji Joshi) located in Sugar Land, Texas (a suburb of Houston) and Mtleshkumar Patel and Rajubhai Patel located in Willowbrook, Illinois (a suburb of Chicago).
20 TIGTA Semiannual Report to Congress (March, 2015) at 54.
21 TIGTA Semiannual Report to Congress (March, 2016) at 40.
When TIGTA further reported that it had, “… shut down 431 of the 574 telephone numbers used by the scammers,”22 it’s easy to see what happened next. The fraud mutated. It went into the Internet, and deeper into technology. CP-2000s were mail-merged with a victim’s identity information and then delivered by e-mail. A new scam was born on the ashes of the old.

It is noteworthy how swiftly and broadly the new e-mail scam took hold. This tells us something important. Agility like this is common when organized crime becomes engaged in tax fraud. The same kinds of mutation and migration patterns can be seen in a number of European Union (EU) frauds. In particular, fraudsters in the EU have been engaged in massive, highly organized missing trader (MT) frauds in the value added tax (VAT). Many of these frauds (like the phone scams and e-mail scams in the US) are remotely controlled from outside the country where they do damage. Some are controlled from as far away as Pakistan, and Afghanistan.

EU MT frauds started with networks of fake businesses selling mobile phones. When enforcement arose in the mobile phone market the fraud quickly mutated. New fake networks began selling computer chips in grand circles (carousels) to steal VAT refunds. When the computer chip fraudsters were pursued the fraud mutated (again) and moved deeper into technology. Most recently MT frauds involve the sale of hard to trace (but easy to transfer) intangible commodities like VoIP calling rights, and CO2 emission permits. EU losses are in the hundreds of billions of euro annually. MT fraud has become so severe that it threatens to bring down (completely restructure) the EU VAT.23

Because the EU has not adopted the technology solutions at hand, for example blockchain (distributed ledger) technology,24 or a Bitcoin (VATCoin) solution,25 the EU enforcement efforts are hamstrung. Gumshoe, traditional audits predominate. The frauds continue to mutate. Huge legal and audit resources are pumped into global searches for elusive masterminds who direct the fraud’s foot soldiers from abroad.

Both the Italian26 and Russian27 mafia are known to be engaged in MT frauds along with terrorist groups like Al-Qaeda,28 and the Islamic State (ISIS).29 Is something

---

22 TIGTA worked with the phone companies to try to resolve the phone scams.

To protect taxpayers from being victimized by the scammers TIGTA established an “Advise and Disrupt” approach to the scam that identifies the telephone numbers used by the scammers and, through an automated process, calls those telephone numbers to advise those scammers that their activity is fraudulent and criminal.

TIGTA Semiannual Report to Congress (March, 2016) at 3 and 41.


24 Richard T. Ainsworth & Andrew Shact, Blockchain Technology Might Solve VAT Fraud, 83 TAX NOTES INTERNATIONAL 1165 (September 26, 2016).


26 Richard T. Ainsworth, The Italian Job – Voice Over Internet Protocol MTIC Fraud in Italy, 58 Tax Notes International 721, 733 (May 31, 2010) (discussing the involvement of the Ndrangheta mafia (a crime
comparable happening in the US? Who is really behind these highly organized US scams? Is it an enterprising individual in India or a known organized crime group? We are clearly witnessing a series of orchestrated attacks on the US tax system. Can we stop it?

Are the masterminds located where the phone lines end (in India), as suggested in the HGlobal indictment? The American tax system has been scammed before to fund terrorist groups. Hezbollah used sales suppression frauds and cigarette smuggling in the US to fund its activities. Is it happening again?

THE FRAUDS RELY ON SPEED

Technology-based frauds place a premium on speed. Transactions happen fast, money changes hands fast, and everything is designed to collapse and evaporate on a moment’s notice. Traditional audit techniques are no match for technology. The trail to the mastermind is gone almost as soon as it is walked upon. The real organizers are hidden behind row upon row of expendable operatives who are paid a small percent of the funds passing through their hands.

The scammers made thousands of calls and used technology to hide where the calls were coming from and where the victims’ payments were being sent.

syndicate from the toe of the Italian boot) in a tax fraud constructed around VoIP and a money laundering operation, the funds for which came from an earlier MTIC fraud in cell phones).

27 Ashley Seager & Ian Cobain, Carousel Fraud: Bogus Deals keep Customs in a Spin: Smart Criminals Stay Ahead of Investigators Russian Mafia and IRA Linked to Swindles, THE GUARDIAN (May 9, 2006) (discussing through interviews how the Russian mafia push into a cell phone MTIC fraud operation run by two Englishmen and took over).

28 Staff report, Italy Tax Scam “may have funded terrorism,” THE LOCAL (September 24, 2014) available at: http://www.theflocal.it/20140924/1bn-italy-tax-scamp-may-have-funded-terrorism (describing Italian reports by the Milan prosecutor that a €1.15 billion tax scam involving the trade of carbon credits through Italy may have financed terrorism based on documents found at the Afghanistan/Pakistan border by US and UK special forces pursuing Osama bin Laden before he was killed in 2011); Luigi Giuseppe Guastella Ferrarella, The Great Scam of VAT in Italy to Finance Islamic Groups, CORRIERE DELLA SERE (September 24, 2014) available at: http://www.corriere.it/cronache/14_settembre_24/grande-truffa-dell-iva-italia-finanziare-gruppi-islamici-ec394336-43a5-11e4-bbc2-282fa2f68a02.shtml?refresh_ce (in Italian)

29 Bo Elkjaer, Troels Kingo Larsen & Mads Nilson, Terror Suspects involved in Food Fraud in Copenhagen, DR (January 25, 2016) available at: http://www.dr.dk/nyheder/terremistaenkte-indblandet-i-foedevarefusk-i-koebenhavn (describing terrorist suspects acting as directors of Danish firms participating in VAT frauds in soft drinks, chocolate and frozen chickens who funneled the funds to the Islamic State and Al Qaida while supporting Spanish recruitment of fighters under investigation by Spanish authorities) (in Danish).


An investigation of the phone scam conducted by the Pindrop Security Blog, published on April 14, 2014 is eye-opening. In less than 30 days Pindrop tracked the fraud that became the Houston indictment two years later. TIGTA’s March 2014 semi-annual Report to Congress was the first official (public) report of the phone scam in the US. Pindrop decided to test TIGTA’s statements the next month. It indicated:

The IRS is warning people about the “largest ever” phone fraud scam targeting taxpayers. In the interest of learning more about this phone-based threat, Pindrop has investigated the attacks …

Findings:

- Attackers are using MagicJack VoIP phone numbers for consumers to “call back” as part of this attack. …
- The attackers appear to be operating out of India and are seeking approximately $5,000 per successful attack.
- The attackers are asking consumers to use GreenDot Money-Pak service to wire money to a PayPal account.
- As compared with previous attacks involving impersonation of the IRS, this attack involves much higher volumes, with complaints in excess of 10 times higher than previously seen. We estimate the number of attack calls has already exceeded 450,000 in March [2014].

Given that the US “ringleader” (Sahil Patel) was arrested on December 18, 2013, the following two charts by Pindrop are interesting. In the first chart Pindrop graphs the MagicJack VoIP phone numbers used by the fraudsters up through April 2014. Rather than decreasing immediately after the arrest of Sahil Patel, the Pindrop records show that the phone calls increased almost “off the charts.”

This suggests that rather than running and hiding after the alleged US “ringleader” was arrested and the fraud was substantially uncovered, the true masterminds “doubled down” on the US phone scam, and tried to squeeze every last dollar out of the American public before moving on.

---


33 MagicJack is an inexpensive, online VoIP service. Pindrop accurately determined that the fraudsters were using this service in 2014. This is the same conclusion reached by the Grand Jury in the HGlobal indictment, which indicated that 1,500 MagicJack numbers were used. MagicJack numbers organize large portions of the indictment. For example (713) 370-3224 MagicJack was registered in the name of an individual in Waco, Texas (stolen identity) by individuals in Ahmedbad, Gujarat, India. It was used to access more than 4,000 General Purpose Reloading (GPR) cards to transfer funds from other cards registered in the names of over 1,200 different misappropriated identities in the year 2013.
The second chart of interest is the time distribution of the calls. It is clear that this scam is working on Central and Eastern Time. This suggests that the Indian call centers are being closely coordinated with US operatives. The four US domestic managers are located in the same time zones (two are living outside of Chicago, Illinois, and two are living outside of Houston, Texas). Are the masterminds in the US or outside the country? The Grand Jury states that the phone scam was planned and “… organized by conspirators in India.” This makes everyone in the US a foot soldier. Real control is elsewhere.

The Pindrop charts make sense. Foot soldiers do not “double down” (of their own volition) when they are engaged in a visible fraud, and they certainly do not do that at the moment when the police are knocking at the door arresting supervisors. Foot soldiers “double down” like this when they are ignorant of what is going on, and when they are tightly controlled from above. Pindrop found and published in one month (April 15, 2014 – tax day) what the Grand Jury only announced in October of 2016.

---

34 US Attorney, Southern District of Texas, *Dozens of Individuals Indicted in Multimillion-Dollar Indian Call Center Scam Targeting U.S. Victims*, (October 27, 2016) available at: https://www.justice.gov/usao-sdtx/pr/dozens-individuals-indicted-multimillion-dollar-indian-call-center-scam-targeting-us. *US v. HGlobal* is the result of a multi-agency, three-year investigation into the phone scams that brought 61 individuals and entities to court on criminal conspiracy, wire fraud and money laundering charges. This case is going to trial in the Southern District of Texas, Houston Division and involves 20 individuals arrested in the US, 32 others in India along with 5 Indian call centers.
In the March 2016 *Semiannual Report to Congress* TIGTA reported that it had shut down 431 of the 574 telephone numbers used by the phone scammers. By the time of this announcement the phone scam had already *migrated* to Canada and the UK. The US was in the midst of different scam, the *CP-2000 e-mail scam*.

The scam morphed from phone calls to e-mails, but the essential problem for the American citizen remained the same. The Taxpayer’s problem is that under either of these scams the fraudsters are placing him under pressure to respond to an apparent message from the IRS which is threatening imminent arrest, seizure of assets, or worse. How can the validity of this message be verified? How can it be done simply, quickly, and authoritatively?

In the case of the *CP-2000 e-mail scams* the IRS advice is to scrutinize the CP-2000 notice that was received, and try to identify it as fraudulent. The IRS says the first thing the Taxpayer should do is compare the CP-2000 they received with a real CP-2000 printed in the IRS document *Understanding Your CP2000 Notice*. This document is posted on the web.

In addition, the taxpayer should look for the following signs of fraud in the document it has received:
(a) the false CP-2000 notice will appear to be issued from an Austin, Texas address;
(b) the unreported issue will be related to the Affordable Care Act (ACA) requesting information regarding 2014 coverage;
(c) the payment voucher will list the letter number as 105C
(d) the taxpayer will be requested to make a payment with a check made out to “I.R.S.” at the “Austin Processing Center” and at a post office box (a true CP-2000 asks that a check be made out to the “United States Treasury”);
(e) an additional “payment” link will be embedded in the e-mail itself.35

This advice is not simple, nor can a stressed taxpayer do it quickly. It is however, very similar to the advice offered by the HMRC in the UK,36 or the CRA in Canada when their taxpayers receive similar fraudulent notices from scammers.37 There is a better way.

THE DUBAI SOLUTION

Dubai does not have a modern tax system. It relies on a 55% tax on oil and gas company profits, and a 20% tax on the income of foreign banks. A 5% VAT is planned for January 1, 2018.

Residents do make regular payments to the government for utilities. Invoices for usage are mailed to residents on paper, and e-mail. The distinctive part of each communication is the QR code placed on each communication. Residents scan the QR code to verify the invoice with a government provided app. The verification procedure is the same process used by WhatsApp for Web.38 The Dubai app also facilitates direct payment, if the resident links the app to a bank account.

THE APPLICATION

Adapting the Dubai Solution to the US phone scams and e-mail scams would be relatively easy. There are six steps (and an optional seventh step):

STEP ONE: The IRS would use an official government web site through which any citizen could download the security app. The app is downloaded within the user account of the IRS web site, and not from an app store.

STEP TWO: The user would be presented with a SSL (Secure Socket Layer) certificate from a verified certificate authority. The certificate would show that the web site is the correct IRS web site and not a web site set up by criminals to look like the IRS site. Whenever a citizen would go to this web site through the app the web site would display a known symbol or picture to the user.

STEP THREE: Every IRS document (whether issued on paper, as an e-mail, or through an attachment to an e-mail) would contain a QR (Quick Response Code) code.

STEP FOUR: There are two QR codes used in each verification transaction. One is on the paper document, e-mail, or e-mail attachment in the hands of the citizen; the other is on the IRS web site.

STEP FIVE: The function of the app on the smart phone is to test the two QR codes as a key pair.

STEP SIX: Within less than a second, the app will return to the citizen document verification.

STEP SEVEN: If the government is interested in policing this fraud area more thoroughly it could (in instances where the app rejected the pairing of the QR codes) allow the citizen to submit a digital notification to the IRS that an individual impersonating an IRS officer had attempted fraud. There could be a “whistle blower” award attached to this notification.

IRS ADVICE TO TAXPAYERS WHO SUSPECT FRAUD

The IRS would now tell any taxpayer who suspected fraud in any communication, which allegedly came from the IRS to:

Go to your app and verify the document (or communication).

The advice is simple. The IRS will say the same thing and have the same answer regardless of the fraud attempted. Repeated announcements will make the solution second nature to the taxpaying public. Thus:

(1) If an e-mail shows up in a taxpayer’s inbox without a QR code, the taxpayer will immediately recognize it as fraudulent. The taxpayers may want to forward the e-mail on to the IRS through the app for a whistle-blower award. (2) If the e-mail has a QR code, the taxpayer can immediately test the validity of the e-mail with the app.

SSL (Secure Socket Layer) is the standard security technology for establishing an encryption link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private. SSL.Com, Q10241 – FAQ: What is SSL? available at: 
http://info.ssl.com/article.aspx?id=10241

QR (Quick Response) Codes are machine-readable codes consisting of an array of black and white squares, typically used for storing URLs or other information for reading by the camera on a smart phone. Electronic copy available at: https://ssrn.com/abstract=2919060
(3) If there is an e-mail attachment (like a CP-2000) this form should also have a QR code. If there is a QR code the taxpayer should immediately test the document, if not the document is fraudulent, and should be reported.

(4) If a document comes in the regular mail the same process will be repeated. Valid documents will have QR codes on them that can be verified.

(5) If a phone scam is attempted, a taxpayer can immediately access the app and ask through the secure channel if the IRS has an outstanding notice for him that may not have been received. The caller should be asked details about the alleged notice or letter. These details should allow the taxpayer to confirm the veracity of the caller’s assertion.

If the IRS adopts the Dubai Solution, countless follow-up scams can be prevented. If we just consider just IRS notices, there are over a hundred that could be counterfeited, mailed or attached to an e-mail. There are twelve high frequency notices that can easily fit the CP-2000 email scam profile.41

Given that it would take approximately six months to install the Dubai Solution in the IRS, it would seem that the return on investment would be about six to nine months further out. This is indeed the kind of “service” the public expects from the IRS.

41 The most common notices that could be used for this purpose are:
• CP 12 - The IRS made changes to correct a miscalculation on a return.
• CP 14 - First notice that a balance is due.
• CP 31 - A refund check was returned to the IRS. Need to update address.
• CP 42 - The amount of a refund has changed because the IRS used it to pay a spouse's past due tax debt.
• CP 49 - All or part of a refund was used to pay a tax debt.
• CP 90/CP 297 - Final notice -- notice of intent to levy and notice of the taxpayer's right to a hearing.
• CP 91/CP 298 - Final notice before levy on Social Security benefits.
• CP 161 - Request for payment or notice of unpaid balance.
• CP 501 - First reminder notice that there is a balance due.
• CP 503 - Second reminder notice that there is a balance due.
• CP 504 - Final balance due notice. If amount is not paid immediately, the IRS will seize (levy) a state tax refund and search for other assets to levy.
• CP 523 - Notice of default on installment agreement and imminent seizure (levy) of assets.