Shell games
Investigating shell companies and understanding their roles in international fraud

RYAN C. HUBBS, CFE, CIA, PHR, CCSA
July/August 2014

Criminals use shell companies to launder money, evade taxes and perpetuate all manner of fraud. The author defines and dissects shell companies to help CFEs investigate this threat that can hit uncomfortably close to home.

For many anti-fraud professionals, the thought of having to investigate, understand or come face-to-face with a shell company scheme may seem remote at best. We may hear about shell companies on the news. But that happens to other companies, in other countries, in other industries, right?

Unfortunately, the landscape of international crime and fraud has changed dramatically in the last quarter century. Shell companies aren't just for big tax evaders anymore. If your organization is engaging in any type of transaction in today's economy, shell companies should be a concern. They're the financial and deception vehicle of choice for some of the most corrupt, dangerous and ruthless individuals and entities in the world. Arms dealers, drug cartels, corrupt politicians, scammers, terrorists and cybercriminals are just a few of the frequent users of shells. Saddam Hussein, Iran, Al Qaeda and Osama bin Laden are, or were, some of the fans of shell companies. (See Web of Shell Companies Veils Trade by Iran's Ships by Jo Becker, New York Times, June 7, 2010.) Not to be outdone, legitimate business entities are getting into the international shell game, and some are unfortunately proving to be very good at it.

In April of 2014, Hewlett-Packard agreed to pay more than $100 million in criminal and regulatory penalties to the U.S. Department of Justice and Securities and Exchange Commission. According to Deputy Assistant Attorney General Bruce Swartz, “Hewlett-Packard subsidiaries created a slush fund for bribe payments, set up an intricate web of shell companies and bank accounts to launder money, employed two sets of books to track bribe recipients, and used anonymous e-mail accounts and prepaid mobile telephones to arrange covert meetings to hand over bags of cash.” (See the April 9, 2014, U.S. Department of Justice release, Hewlett-Packard Russia Agrees to Plead Guilty to Foreign Bribery.)

Not all shell companies are used for nefarious means; there are legitimate uses for these entities, such as using one as a holding company or creating a shell company (in name) to preserve future business rights or opportunities. Not every shell is involved in a criminal conspiracy, so it's important to understand why someone might use a shell for criminal purposes. The primary purpose is like any other basic fraud scheme: to conceal. This may include the nature, origin, or destination of misappropriated funds and/or concealment of the true owners and decision-makers of a criminal act or conspiracy.

SHELL, SHELF AND INCORPORATORS

In many instances, one shell company isn't enough — fraudsters need a network. Dozens of shells, nominee directors, addresses and fake shareholders might be required to conceal a scheme or criminal plot. Big-time criminal conspirators will utilize shell incorporators to do the heavy lifting and help create a corporate web of disguise that can perplex and confuse the best of investigators. Shells can come in different shapes and sizes, and the jurisdiction in which they reside can help further the concealment.

Some fraudsters create shell companies for single uses and then discard them. Or they may use them repeatedly and have them change hands multiple times. They also may form "shelf companies" and not use them for a period of time. A shelf company has a better chance of appearing legitimate and fooling a novice investigator or basic due diligence mechanisms because it appears to have existed longer than it really has. An older shelf could predate any specific areas of concern, which would allow it to engage in business activities when it otherwise shouldn't.
There are literally hundreds of listed shell incorporators on the Internet and around the world. One of the most widely used incorporators is Wyoming Corporate Services, a shell/shell incorporator located in Wyoming. According to a Reuters news investigation in 2011, several shell companies originating at this location have been used in numerous international frauds and criminal activity. (See the Reuters June 28, 2011, article, Special Report: A little house of secrets on the Great Plains, by Kelly Carr and Brian Grow.)

Some shell incorporators are more secretive and selective with whom they do business than others. Regardless, with a small sum of money, time and patience, fraudsters can set up a very elaborate web of shell companies in little time. But establishing the company name is only the first step in creating a shell network of deception. The company needs nominee directors and shareholders — often illegitimate — to further the concealment.

SHELL NOMINEE DIRECTORS

Fraudsters use nominee directors, and in some instances, other shell companies, to disguise true owners of entities while giving the appearance of legitimacy. Some nominees simply sell their names to fraudsters who use them on company documents. Others actually provide limited services for the shell companies such as processing corporate records, signing for company documents and forwarding mail.

Numerous organizations have been working to uncover the network of nominee directors. The U.K. Guardian newspaper, with the assistance of other international investigative and anti-corruption organizations, has identified that a mere 28 nominee directors have set up and/or are in control of more than 21,000 companies — many of which have been identified as being involved with criminal organizations/individuals. (See The Guardian blog article Offshore secrets: how many companies do “sham directors” control? by James Ball, Nov. 26, 2012.) A simple Internet search of some of these nominee directors easily links their association with frauds such as the United Nations Oil for Food Program, Mafia operations in Italy and numerous instances of money laundering.

These nominee directors are the linchpins to linking and disguising international criminal organizations and operatives. Their use is so widespread that within a few searches among entities, these nominee directors cross paths. Some are even listed as directors for the same entities. In early 2014, The International Consortium of Investigative Journalists (ICIJ) published a graphical interface of the incorporation records of shell companies, directors and addresses that were leaked to them on two shell incorporators. Their database illustrates the extent of some shell company networks and how many companies, individuals and nominee directors are linked together. (Search the ICIJ offshore leaks database.)

SHELL INCORPORATION HOTSPOTS

In June 2012, Global Witness, an international anti-corruption organization, published a report, "Grave Secrecy," which documented the shell companies and international criminal networks in and around Russia and Kyrgyzstan that were involved in money laundering, corruption and fraud. "In one case, the identity of a dead man from Russia was used as the front for a UK company. While this person had died three years before the company was set up, he was listed as the company’s owner and he even ‘attended’ a company meeting in London," stated the report.

Global Witnesses’ investigation identified more than 20 companies that at first glance didn’t appear connected to one another. But a detailed review of the directors, connections and business addresses yielded a very large interconnected network that spanned several countries. (Read the PDF of the full report, Grave Secrecy.)

One of the address hotspots identified in the Grave Secrecy report was "103 Sham Peng Tong Plaza" in Victoria, Seychelles. A simple Google search of this address identifies more than 160,000 hits associated with websites, companies and individuals. Another address identified in unrelated criminal filings and sanctions is P.O.Box 3444 Road Town, Tortola, BVI. A Google search of this address yields more than 600,000 hits. These addresses represent just a few incorporation hot spots. An entity identified with one of these addresses should be a huge red flag.

INVESTIGATING AND TRACKING SHELLS VIA THE INTERNET

The main purpose of using a shell is concealment. So, tracing and tracking shell companies to their owners isn’t easy, but it’s not impossible either. The following tools and techniques can significantly help the anti-fraud professional in verifying a shell, or at the very least, help uncover that one piece of information that could unravel the entire shell network.

1. Web history

Fraudsters who want to establish shells, of course, must have websites to create the appearance of legitimate companies. Sometimes bad actors get sloppy and put too much information on a website or list information that can then be linked to other entities that they control or oversee. One extremely useful tool, archive.org, takes snapshots of most websites on the Internet. Even if the website has changed or is no longer being hosted, you may find useful available historical information. These snapshots may help verify known information or point you in a new direction.

2. Public records to identify owners and tracking to known associates

Public records are an important key to help link entities and individuals together. Some public records sources require paid subscriptions like LexisNexis or CLEAR, while some others provide public records for free, including www.opencorporates.com, ICIJ Database, the Panama Free Search Database, and CompanyCheck for the U.K.

As you uncover information, you should continue tracing the shell to all known associates to help uncover and map the network. Continue to chase down and cross-reference all leads, contacts and sources to get
3. Mapping the network

The most important task for tracing and tracking shell companies and contacts is to be able to document the linkage between all the information uncovered. The amount of leads, dead ends and information can be overwhelming; a single piece of important information could go unnoticed or unlinked. Most investigators can't afford expensive mapping technologies. The next best option is a free online mapping and relationship tool, www.draw.io, which investigators can use to create easy relationship diagrams for presentations and reports and keep track of inter-related connections. Map every piece of information — no matter how small. An address or phone number could be the key to uncovering the shell network. Search online for various combinations of phone numbers and addresses.

4. ‘Whois lookup,’ for domain ownership, IP addresses

Shell incorporators might have been vigilant in concealing public records’ information on involved entities, but they may have been careless when setting up the corresponding website addresses. Using "Whois lookup" search engines, you can discover:

- Domain ownership
- IP addresses.
- Physical addresses of websites.
- Website administrators and their contact information.
- Website creation dates.

Hundreds of Whois websites are available. One site, whoisology.com, provides linkage analytics by linking all websites in its database based on characteristics, names and fields. Want to know how many websites are located at the shell incorporation hot spot address of “103 Sham Peng Tong Plaza?” As of April 2014, Whoisology reports that there are more than 900.

5. Evaluating online presence

Shell incorporators have a hard time faking an active and robust online presence because these companies technically don’t exist. What constitutes a robust online presence?

- The existence of a well-designed website.
- The presence of other online content.
- Periodic and regular updates of information.
- Contact email addresses that are linked to a legitimate website address, not free email accounts.

How do shell incorporators try to get over this hurdle and make their business look more legitimate?

- They often post company and contact info on numerous free 411 sites, which are online white/yellow pages.
- They might create placeholder websites to get domain specific email addresses, such as brad.johnson@placeholder.com.
- They often create fake social media profiles for the company and its "employees."

As you vet an entity, ask these questions:

- No online presence whatsoever? (Huge red flag.)
- Is the amount of online information available consistent with the goods/services that the entity says that it's engaged in?
- Is there too much free online posting of information on the company?

OFFSHORE COUNTRIES AND BANKS

A shell company can be set up practically anywhere, but incorporators widely use particular countries and regions. Advantages can include lack of government enforcement or specific laws protecting corporate secrecy. A good source of a high-risk country list is the U.S. State Department's annual list of major money-laundering countries.

You can identify bank-specific SWIFT codes in high-risk countries with a website such as theswiftcodes.com. (A SWIFT code is a unique identifier that's associated with financial and non-financial institutions around the world.) After you identify the SWIFT codes, you might want to monitor for any funds originating or being disbursed to these banks or check to see if any customers/vendors have banking accounts associated with these specific banks.

IDENTIFYING YOUR RISKS: REVIEWING AND MONITORING YOUR INTERNAL DATA

The evidence is clear: Shell companies exist, they are plentiful, and their connections and networks can be vast. Depending on the size and international breadth of your organization, it could be a victim or an unwitting pawn. Reviewing and monitoring your internal data will reduce your risk of involvement with a shell.

1. What do I need to review?

Review all available internal data that contains contact, banking, address and ownership information, such as vendor/customer data, wire transfer data, ship to/ship from locations for sales and purchases, purchase orders and invoice support documentation.

2. What should I be looking for?

- Information that doesn't make sense given the nature of the business relationship with the entity.
- Entity information mismatch: address, phone, fax, ship to, bank, cell contact, etc. in different geographic locations.
No discernable online presence when compared to the goods/services and the amount of money changing hands.

The entity "representative" is associated with numerous other companies.

Payment is made to or received from an unrelated third party. (Review incoming/outgoing wire transfer documents.)

ONLINE RESOURCES

Tracking, tracing and investigating shell companies can be time consuming and difficult without resources and assistance. These online organizations are involved in various aspects of investigating, reporting and/or tracking shell companies and criminal organizations:

- Financial Crimes Enforcement Network (FinCen)
- Office of Foreign Assets Control (OFAC)
- International Consortium of Investigative Journalists (ICIJ)
- Global Witness
- Financial Action Task Force (FATF)
- The Guardian
- Offshore Alert

DON'T BE A PLAYER IN THE WORST GAME IN TOWN

Shell companies and those associated with them can be very bad news for a company. Fraudsters within your organization might use them as vehicles of corruption or asset diversion. External perpetrators can passively use them as money-laundering vehicles against your organization.

Stay current with the latest on shell companies, international corruption, fraud and asset diversion, and money laundering. Screen information on your customers, vendors and employees. Cross-reference known bad actors and shell companies against the entities with which you're doing business. Contact authorities if you're the victim of a shell company scheme.

Stay vigilant! The shell company that's being organized today could be the center of the next big international fraud of tomorrow. Don't let your organization have front row seats to the worst game in town.

Ryan C. Hubbs, CFE, CIA, PHR, CCSA, is the forensic audit manager for Halliburton in Houston, Texas. He's a member of the ACFE faculty.

Read more insight and discuss this article in the ACFE’s LinkedIn group.

The Association of Certified Fraud Examiners assumes sole copyright of any article published on www.Fraud-Magazine.com or www.ACFE.com. ACFE follows a policy of exclusive publication. Permission of the publisher is required before an article can be copied or reproduced. Requests for reprinting an article in any form must be emailed to FraudMagazine@ACFE.com.
Reviews

By Michael_22

By Danielle_Cheek

By Ryan_Hubbs_3

By Manish_Jain

By Patrick_34

By Will_Nelson