MŰSZAKI KATONAI KÖZLÖNY
A MHTT Műszaki Szakosztály és a ZMNE folyóirata XXI. évfolyam, különszám,
2011.december

ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM

VÉDELMI IGAZGATÁS SZAK

A Magyar Tudomány Ünnepe rendezvénysorozat keretében a

„Hallgatók a Tudomány Szolgálatában”

Védelmi igazgatás szakos hallgatók

IV. országos tudományos konferenciája

Veres Viktoria:

Bűnözés katasztrófák idején: az áldozatok és adományozók pénzügyi megkárosítása

Disaster fraud: financial crime committed against disaster Victims and donators

Budapest, 2011. november 10.

Abstract

Az elmúlt évek katasztrófai során megtapasztalhattuk a katasztrófák pusztításának egyre erőteljesebb következményeit, kevés szó esik azonban a katasztrófák utáni időszakokban megjelenő újabb es újabb bűnözői csoportokról és a megkárosítás módszereiről. Nemcsak a katasztrófák áldozatainak kiszolgáltatott helyzete ad számos lehetőséget bűnözőknek és csalóknak, hanem a társadalmi felelősséget érző emberek segítőkészsége és adományozó készsége, valamint az egyre szaporodó non-profit szervezetek működése is.

A szerző ebben a tanulmányban vizsgálja a katasztrófák áldozatainak és az adományozók pénzügyi megkárosításának lehetőségeit, úgy mint a személyes- és pénzügyi adatok eltulajdonítása és felhasználása, hamis vagy tisztességtelen szerződések kötése, pénzösszegek kicsalása interneten terjesztett vagy személyes megkeresésen alapuló, nem létező vagy az adományokat nem megfelelő módon felhasználó non-profit szervezetek nevében, valamint az adományozás felhasználása pénzmosás, terrorizmus finanszírozás vagy adókerülés céljára. A szerző arra hívja fel a figyelmet, hogy katasztrófák után segítséget elfogadni elkerülhetetlen, a pénzügyi adakozás és segítségnyújtás pedig az egyik meghatározó eleme a felkészülésnek, mentésnek es újjáépítésnek, ugyanakkor fontos, hogy megtanuljuk, hogyan kerülhetjük el, hogy csalók áldozatává váljunk vagy akaratlanul is támogassuk a bűnözést, és hogy adományaink a legjobban rászorulókhoz jussanak.

Kulcsszavak: katasztrófa, bűnözés, pénzügyi csalás, adományozás, non-profit szervezetek

Keywords: disaster, crime, financial fraud, donation, charities

INTRODUCTION

We all learned, saw or experienced how disasters destroy human life and property all over the world. Experts do significant efforts to reduce vulnerability and losses in the 4 main phases of the disaster management (mitigation, preparedness, response and recovery). This article outlines a specific problem that occurs mainly at disaster response and recovery while drawing attention to the importance to raise public awareness as part of disaster mitigation and

preparedness programs. Just like the growing frequency and intensity of disasters, the complexity, occurrence and volume of fraud and crime committed during disaster time is increasing. This article examines the main types of financial abuse, fraud and crime committed in connection with disasters and gives examples form worldwide and why can people be victimized easier during and after disasters.

Disasters may cause unforeseen physical danger, psychological trauma and losses[43] to the people affected along with short and long term financial needs for recovery afterwards. As a result victims are more vulnerable to be abused by criminals. On the other hand people who were not directly affected by disasters, but would like to help disaster victims by making various donations can also fall victim to criminals. Moreover, disaster related matters can open ways for supporting Money Laundering and Terrorist Financing or Tax Evasion.

Hurricane Kathrina, earthquakes in Haiti and Pakistan, Oil Spills at Deepwater Horizon and the Tsunami in Japan[44] all required advanced collaboration from governments, national and local institutions to investigate fraud, waste, abuse, or mismanagement and take necessary actions. As an example, in the U.S. after Kathrina a record number of possible fraud was reported and investigated: `The command center, now known as the National Center for Disaster Fraud (NCDF), has received and screened more than 46,000 complaints of disaster fraud and referred more than 30,000 of those to law enforcement for investigation.`[45] and that `the Department of Justice has charged more than 1,300 defendants in 47 judicial districts throughout the country for disaster fraud related to Hurricanes Katrina, Rita, and Wilma, the Gulf Coast oil spill, and other disasters.`[46]

---

[43] Dr. Hornyacsek Júlia: A tömegkatasztrófák pszichés következményei, és az ellenük való védekezés lehetőségei, in: Bolyai Szemle 2010.XIX. évfolyam 4. sz. ZMNE Budapest: 2010. 5. oldal. ISSN: 1416-1443

[44] Interesting addiction that according to some news providers in Japan after the tsunami even a crime group has delivered donations to the victims: http://articles.businessinsider.com/2011-03-18/news/30056980_1_kai-crime-group-supplies (4/11/2011)

[45] http://www.fbi.gov/birmingham/press-releases/2011/national-disaster-fraud-hotline-available-to-report-storm-related-fraud National Disaster Fraud Hotline Available to Report Storm Related Fraud FBI U.S. Attorney`s Office (2/9/2011)

[46] Same as above

Raising awareness to report disaster fraud
Poster: http://www.dhs.gov/xoig/assets/DHS_OIG_Hotline_Fraud.pdf

There are plenty of ways to fraud people; we can categorize crime committed in time of disasters various ways. For the purpose of this article considering the limited space and the complexity of the topic (taken only the funds related abuse) the categorization is according to the target group and participants of the disaster crime:

1. Fraud/Crime committed against disaster victims and their properties (Identity or/and Financial Information Theft, Credit Fraud, Contractor Frauds and Government Loans, etc)
2. Fraud/Crime committed against people who would like help disaster victims (False Donations, Credit Fraud, Identity or/and Financial Information Theft, etc)
3. Fraud/Crime committed using and abusing charity organizations (Money Laundering, Tax Evasion, etc)
4. Fraud/Crime other than the above (False Damage Claims, etc) that is subject of further examination

1. ABUSE OF DISASTER VICTIMS

1.1 Identity Theft and Related Financial Fraud

During and shortly after disasters there are plenty of opportunities for thefts to enter into abandoned properties and access personal items that can be abused in various ways. Ad hoc fraudsters take advantage of unsecured homes and businesses, and more and more often they do it planned and organized. Their goal is to access personal information, identity documents, utility bills, credit cards, electronic banking information, signature samples and numerous other kinds of proofs that will help them to impersonalize disaster victims.

Having these details can lead among other to:

1. **Unauthorized credit transactions**, such us criminals taking money from the found credit card or electronic banking transactions of the victims
2. Taking commercial **loans in the name of the victim**
3. Using the **victim`s details, pictures to collect donations**
4. Using victims details to **access government funds,** loans or other donations[47]
5. Other

During and after disasters many time victims need to give their personal details to rescue organizations, reconstruction and home repair companies, insurance agencies, therefore criminals can retrieve personal information not only by entering into unsecured properties during disasters but by acting as members of these organizations.

Whenever it is possible, giving personal information shall be only after we are sure that a legit person and organization is requesting and using it. When governmental and insurance scam artists appear at victims` houses to collect personal, banking, insurance information, social security number it is hard to identify scams.[48] A good indicator of fraud can be that real organizations never `push` to answer, never express the disadvantages of not giving information to them, never ask for credit card and banking passwords, never refuse or tell

[47] http://www.fbi.gov/birmingham/press-releases/2011/federal-grand-jury-returns-three-disaster-fraud-indictments Federal Grand Jury Returns Three Disaster Fraud Indictments FBI (4/11/2011)

48 http://www.fema.gov/news/newsrelease.fema?id=55070 Arkansans Warned To Watch Out For Scam Artists. FEMA (4/11/2011)

excuses of not having their identity document with them and never promises that by providing details they can arrange quicker disaster assistance and more financial help for disaster victims.

If there is no option to check the organization or the person requesting information, when giving sensitive details it can be useful to **keep record of when, where, what information has been provided**.

Attempts of scamming though the Internet and emails are part of our everyday life. Even in normal situations many fall victim to these abuses. Along disasters the number of these attempts can multiple and so can be the number of victims who answer to these emails and give their personal and financial details.

It is recommended that disaster victims as soon as possible

- Check their personal and financial documents (ID, utility bills, chequebooks, credit cards, any kind of contract that contains sensitive information), if missing report it immediately to the relevant authorities
- Review their financial history[49] (credit cards, bank, eWallet statements) as soon as possible in order to be aware the earliest if they have been abused, at most of the banks and other financial institutions chargeback can be performed if the transaction is proven to be unauthorized. Further actions such as fraud alerts, credit freezes can differ based on the country law and the financial institutions rules.[50]
- Check if their names and details appear on the internet site collecting donations to `help them`, if it does report it immediately to the relevant authorities
- When governmental loans and other returnable financial help is available after disasters, check with these organizations weather an unauthorized loan was taken using their details

It is extremely important that payment institutions, online services and eShops **examine transactions and orders with due diligence** where the residential address of the buyer is in the disaster affected area. Especially transactions with no economic sense (does not

[49] http://texashelp.tamu.edu/011-disaster-by-stage/recovery/ER-034-Preventing-Fraud-Following-Disasters.php Preventing fraud following disasters. Texas Extension Disaster Education Network (4/11/2011)

meet rescue or recovery needs) in an emergency situation, shall draw the attention of responsible companies that identity theft and unauthorized transaction might have taken place. Hurricane victims ordering expensive jewelry with the shortest delivery date or making online high risk investments is likely to be fraud using stolen or hacked funds. By being suspicious during and after disasters **companies can help credit fraud victims** and also to reduce their own credit risks and losses of chargebacks.

1.2 Scammers asking for cash advance or fee for the services

Scam artist who arrive to disaster victims` houses may not only seek for information that will allow them to use the victim`s identity but also may act as government agents, insurance agents, lawyers, accountants to ask for cash advance payment or service fee for the assistance. The rules can be different country by country, organization by organization but **government officers and insurance agents usually don't accept cash** and mainly they verify the damage only. It is recommended not to pay any fee in our house and to check if the service is free or there is indeed a fee for it. If the fee and the amount are proven from reliable source it is still advised to go to the official office of the organization and pay there.

1.3 Price Gouging, Unfair Contracts, Fake Contractors

People seek quick recovery of their lives after disasters therefore they welcome contractors that shortly offer services after disasters without appropriate due diligence. Disaster victims shall not only be aware of fake contractors, but also legit contractors who abuse disaster victims by **setting unfair prices or contract conditions**. Many governmental websites all over the world warn people from engaging to contracts and giving any personal information before having second or third opinion, price quote and reliable references. The Federal Emergency Management Agency U.S. Department of Homeland security (FEMA) website not even calls for due diligence but states that `Damage visible from the street also can bring out fake contractors who come to your home offering to make repairs. Refuse any offer like that. Most legitimate contractors will have more work than they can handle after a

[50] http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html Defend: recover from identity theft Fighting back against identity theft. Federal Trade Commission (4/11/2011)

disaster.`[51] Also the Interpol raises the possibility of fraud after disasters, lists examples how to avoid fraud constructors and advises not to go into verbal contracts, high loans, not to pay any advance fees before the work has started and to check the contractor`s identity, registration at the company registrar and/or professional associations.[52]

2. ABUSE OF PEOPLE SUPPORTING DISASTER VICTIMS OR DISASTER PREPAREDNESS PROJECTS

2.1 Risks of donating, purpose and methods of criminals

Not only disaster victims can be abused at the times of disasters, but also responsible people who feel solidarity for the victims and would like to help with any form of donations such as goods or financial help are also a target group of criminals. As the Interpol explains criminals are `**Counting on an individual's willingness to help**, and recognizing the difficulties for private citizens to differentiate criminals from legitimate collectors, increasing numbers of criminals are trying to collect donations for their own purposes while impersonating officials of charity organizations.`[53]

The purpose of criminals targeting donators may be among other the following: (a) collecting donations for false use by not using the donated funds for the purpose that was communicated to the donator or is unlawful, (b) credit fraud, a fake non-profit organization or a scam artist simply takes donators funds without any non-profit activity (c) identity or/and financial information fraud, collecting information for future abuse or sale.

The risks of donating and the exposure to fraudulent fund raisers, fake organizations or criminals is determined by the combinations of many factors, such as the subject of the donation (gods or funds), the way and means of donating (traditional personal or electronic), the type of transactions (cash, offline or real time), the frequency and volume of the donations (ad hoc or ongoing, one installment or more installments), use of middle service providers,

[51] http://www.fema.gov/news/newsrelease.fema?id=55070 Arkansans Warned To Watch Out For Scam Artists May 14, 2011. FEMA (4/11/2011)

[52] https://www.interpol.int/Public/FinancialCrime/FinancialFraud/ReconstructionFraud20050107.asp Fraudulent reconstruction tenders and advance fee fraud following natural disasters. Interpol (4/11/2011)

[53] https://www.interpol.int/Public/FinancialCrime/FinancialFraud/DisasterCharityFraud200501.asp Disaster Charity Fraud. Interpol (4/11/2011)

country regulations, awareness of the donators and non-profit organizations on how to identify suspicious situations, etc.

People are likely more vulnerable to fraud if their donations are done using electronic means of **payments over the internet**.[54] On one hand internet or phone based donations using eWallets or Credit Cards are the quickest way to help others all over the world and these transactions may ensure the **anonymity** of the donator. On the other hand these real time online transactions may increase multiple risks of the abuse of personal and financial information and/or that the funds will not reach the intended purpose. Also we tend to fall easier to fraud by doing **ad hoc donations**, seeing and clicking on a banner from our social network or receiving an email with a story of a victim compared to the traditional way when we plan our donations and personally go to the relevant non-profit organization. Incoming e-mails telling stories of victims, asking for donations may also contain viruses and cookies that will track financial info later[55]. The FBI advises us that `Precautions to take include: don't respond to unsolicited incoming e-mails and don't click on links contained within them, as they may contain computer viruses; be wary of people representing themselves as members of charitable organizations and asking for donations via e-mail or social networking sites; make donations directly to known organizations, rather than relying on others to make the donation on your behalf.` [56]

Selling goods (books, leaflets, calendars, etc`) to help disaster victims is also an alternative way of fraud: `An increasing use of the Internet has been noted, whereby offenders promise to donate money from the proceeds made through the normal sale of goods or through **Internet auctions**. Such promises may incite customers to buy even though any donation actually made by the seller may be impossible to confirm.`[57] Anytime when engaging in charity auctions due diligence shall be performed and references of the work of that specific organizer shall be reviewed and confirmed from reliable source.

---

[54] http://www.fbi.gov/news/stories/2005/january/tsunami_scam010505 Tsunami Disaster Relief Fraud Alert! Don't be Scammed. FBI 1/5/2005

[55] http://www.fbi.gov/scams-safety/e-scams/e-scams Haitian Earthquake Relief Fraud Alert. FBI (2/11/2011)

[56] http://www.fbi.gov/birmingham/press-releases/2011/national-disaster-fraud-hotline-available-to-report-storm-related-fraud National Disaster Fraud Hotline Available to Report Storm-Related Fraud. FBI U.S. Attorney's Office May 10, 2011 (4/11/2011)

[57] https://www.interpol.int/Public/FinancialCrime/FinancialFraud/DisasterCharityFraud200501.asp Financial Crime Disaster Charity Fraud. Interpol (4/11/2011)

Fundraisers phoning or coming directly to our house to collect charities or donations can also fraud us using they personal influence, convincing skills and may push us to do immediate decisions, instead of us making our own due diligence on the matter and organization that approached us. Cash payments and Cheques payable to individuals or without name handed over are less track-able for the authorities; therefore it is not recommended to donate by these means.[58]

2.2 Risk of middle systems

Some websites offer **setup systems to receive donations** in 10 minutes[59] without any fee or service charge others offer complex solutions for non-profit organizations[60] in order to help charities to start their fund raising activity as soon as possible and to provide professional assistance. Donators not only shall make sure they know the non-profit organization they are about to support, but also take into consideration the middle-services (payment and security providers, webhosters, etc`) they use, as these service providers may also offer the free service to collect personal or financial information.

2.3 Unfair Insurance Contracts

After disasters people hit or not hit but **influenced by the phenomenon may be easier to be pushed to sign new life-, medical- or property insurance contracts**. Many people influenced by what happened with them or their beloved may sign new contracts with less economic sense or worse conditions then they would do without this experience. Scam artists or unethical insurance agents can take advantage of these fresh bad experiences, losses and fears.

---

[58] http://www.ic3.gov/media/2010/100118.aspx National Center for Disaster Fraud to Coordinate Haitian Fraud Complaints. U.S. Department of Justice Federal Bureau of Investigation18/1/2010 (4/11/2011)
[59] Example of middle service provider: http://www.online.donation.events.org/
[60] Example of complex middle service provider: http://www.donate.net/html2/wwwroot/about_us.asp

3. ABUSING CHARITIES FOR MONEY LAUNDERING AND TERRORIST FINANCING OR TAX EVASION

Regulation of charities[61] is different all over the world, some countries have well defined definitions and strong legal environment, others does not have unified concept on the definition of non-profit organizations or charities but all include the fact that charities have public benefit purpose, not seeking profit and dedicate their activity to charity and help. In most OECD countries (Organisation For Economic Co-Operation And Development Centre For Tax Policy And Administration) fund-raisers and their donators have tax or other benefits upon meeting specific conditions[62] in order to encourage donations. Because of the nature of these organizations, and especially in disaster times or disaster related matters charity organizations can be abused for fraud. The OECD draws our attention to the fact that `Tax evasion and tax fraud through the abuse of charities is a serious and increasing risk in many countries although its impact is variable…The abuse of charities is becoming more organised and more sophisticated.`[63]

Charity organizations can **willingly or unknowingly** (by not knowing that they are used for fraud) **participate in fraud**, such as collecting funds with the purpose to make profit, misusing funds for prohibited activities, issuing receipts that are not based on real donations or issuing fake receipts, giving service or goods in return to the donator, being a `subsidiary` of any profit organization to commit tax or money laundering fraud for the benefit of its members or donators, using charity to collect or transfer fund for terrorist financing purposes. `The abuse of charities occurs when the sanctioned government status of a charitable organization is abused either by the charitable organization, by taxpayers and donors, or third parties, such as fraudsters who pose as charitable organizations or tax return preparers who falsify tax returns to defraud the government.`[64]

---

[61] Definitions of charity organizations can be found in http://www.oecd.org/dataoecd/30/20/42232037.pdf Report On Abuse Of Charities For Money-Laundering And Tax Evasion. Organisation For Economic Co-Operation And Development Centre For Tax Policy And Administration (22/10/2011)

[62] http://www.oecd.org/dataoecd/30/20/42232037.pdf Report On Abuse Of Charities For Money-Laundering And Tax Evasion, Organisation For Economic Co-Operation And Development Centre For Tax Policy And Administration (22/10/2011)

[63] Same as above

[64] Same as above

Donating and social participation at disasters are two key elements for a successful recovery and preparedness. Helping victims must be appreciated and acknowledged by both the public and governments all over the world. `This underlines the importance of knowing that money sent with best intentions is not inadvertently finding its way into the wrong hands.` [65] The fact that charity may open doors for criminals and criminal activity should not dissuade anyone from any sides from this important contribution, especially in disaster times when quick and intensive relief is needed. Even in a very well regulated environment the **responsibility of all sides** is required: (a) the **charity organizations**, (b) the **donors**, (c) the **government** and (d) **companies, banks or payment institutions** in order to avoid criminal activity, some examples will be given below. With proper planning and due diligence a balanced decision can be made so that funds intended to help will reach people in need.

(a) When donating as an individual minimum the following must be seek and considered[66]:

1. Evidence of the existence of the charity (official registrars, visit in the office of the charity, speak to people who already donated, ask for reference)
2. Purpose and geographical spectrum of the organization; local charities with transparent local activity or worldwide well known charities may be easier to observe or account and therefore safer to support than less known charities with far geographical reach.
3. Identifying information on the members and its officers; check government registrars or enquire more information on the membership in National Charity Organization Commission
4. Other publicly available information, such as the organization`s website, other reliable sources, eg. governmental websites, national charity commissions
5. Type, mean, frequency and volume of the donation; preferable use track able methods, such as bank transfers or through reputable service providers, eg. text donation through a well known phone company.
6. Middle service providers

---

[65] http://www.hmrc.gov.uk/mlr/news/pakistan-floods-disaster.htm Pakistan floods disaster - guidance on transmitting money. HM Revenue & Customs (29/10/2011)

[66] Further recommendations can be fund under: http://www.justice.gov/usao/mow/news2011/disaster_fraud_tips.pdf Tips for Identifying or Avoiding Becoming a Victim of Disaster Fraud. FBI (21/10/2011)

(b) When accepting donations as a charity organization

1. Seek for the origin of the funds wherever it is possible, especially at international transactions or transactions from/to high risk countries[67], analyze transactions as per the recommendations of the FATF or any other reputable jurisdiction[68]
2. Perform additional due diligence at big cash (above national thresholds where exists) or anonymous transactions using online payment methods, accepting donations is not a must therefore if the transactions are suspicious deny it and inform the relevant authorities
3. Be suspicious with donations that have terms by the donator, such as saying who or which other organization must be the beneficiary of the donated funds. Report if funds arrived with any other purpose than only charity support, such as anyone willing to send money with the condition that part of the funds shall be refunded, while the rest can be kept by the charity organization.
4. Never respond to requests to issue a tax or other receipt on any different amount than indeed donated. Be aware that some payment methods can be charged back meaning that the donator might reverse the payment even 6-12 months after receiving the receipt to get benefits.
5. Educate employees to identify suspicious transactions and introduce measures and monitoring procedures to prohibit engagement in cooperation with any criminals

The HM Revenue & Customs gives a useful tip for charity organizations to build and increase the trust and confidence of their donators: `Report back to your community so they are reassured that the money has reached the good cause. You may wish to put notices in shops/post offices, or let your local paper know how much you raised and thank people for their support.`[69]

[67] Updated list of high risk countries for Money Laundering and Terrorist Financing can be found on the website of the Financial Action Task Force www.fatf-gafi.org
[68] Example list to identify suspicious transactions can be found under http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/DI144-2007-08.pdf

(c) Governments shall take minimum these steps to avoid the abuse of charities

1. Have a dedicated task force to monitor charity activity, donations and operate additional contacts for reporting possible fraud, have on site visits in the charities offices and/or their activity
2. Introduce regulations and set tax advantages and administrative rules in a way that charities and donations are hard to abuse for money laundering and terrorist financing or tax evasion
3. Ask for specific annual reports and review charity organizations and their donators seeking for specific suspicious patterns, such as sudden high cash donations from a donator that has no history of giving funds to charities
4. Have a registrar of charity organizations, their activity and their members publicly available
5. Educate members of the charity organizations and the public to be conscious when dealing with charity and to be able to identify possible fraud and the ways of reporting it, ensure anonymity of these reports

(d) Other, such as banks and payment services, companies shall do minimum the following when having charities as Clients:

1. Know Your Client: review non-profit clients on a frequent basis, have enough information on the owners, members of the charity and the purpose and geographical outreach of the organization.
2. Perform due diligence on incoming or outgoing transactions that are high in amount and volume and are unusual to the transaction history or geographical outreach of the organization, eg. if the charity that is specialized to support local medical help for children after disasters sends funds to a high risk country for non-medical purposes or seek for explanation when any funds are sent back by the charity to the same source they came form
3. Examine over the counter donations

[69] http://www.charitycommission.gov.uk/RSS/News/pr_pakistan_scam.aspx Be aware of possible Pakistan appeal scams, says Charity Commission. Charity Commission (29/10/2011)

4. Educate employees to identify suspicious transactions and introduce measures to avoid employees cooperating with fraud

SUMMARY

Criminals can approach disaster victims, donators, charities in various ways upon disasters some abusing the victims vulnerability, some the society`s willingness to help, others the tax advantages that governments give to charities. The responsibility to fight fraud is not only on national institutions, police, tax authorities, etc but it relies on all members of charities, donators and also disaster victims. People and companies must not only be thought how to help others in need after disasters but also to be aware for the possible abuse they can face in connection with disaster fraud. This way we can prepare to be conscious on what due diligence to perform before engaging in any activity in any situation connected to disasters from giving personal information, through donations to signing insurance contracts. Invested efforts in raising public awareness on possible scams and fraud as part of the disaster preparation projects and assisting victims after disasters to take deliberate decisions shall return shortly.

INDEX OF REFERENCES*

Dr. Hornyacsek Júlia: A tömegkatasztrófák pszichés következményei, és az ellenük való védekezés lehetőségei, in: Bolyai Szemle 2010.XIX. évfolyam 4. sz. ZMNE Budapest: 2010. 5. oldal. ISSN: 1416-1443

http://www.fbi.gov/birmingham/press-releases/2011/national-disaster-fraud-hotline-available-to-report-storm-related-fraud National Disaster Fraud Hotline Available to Report Storm Related Fraud FBI U.S. Attorney`s Office (2/9/2011)

http://www.fbi.gov/birmingham/press-releases/2011/federal-grand-jury-returns-three-disaster-fraud-indictments Federal Grand Jury Returns Three Disaster Fraud Indictments. FBI (4/11/2011)

http://www.fema.gov/news/newsrelease.fema?id=55070 Arkansans Warned To Watch Out For Scam Artists. FEMA (4/11/2011)

http://texashelp.tamu.edu/011-disaster-by-stage/recovery/ER-034-Preventing-Fraud-Following-Disasters.php Preventing fraud following disasters. Texas Extension Disaster Education Network (4/11/2011)

http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html Defend: recover from identity theft Fighting back against identity theft. Federal Trade Commission (4/11/2011)

https://www.interpol.int/Public/FinancialCrime/FinancialFraud/ReconstructionFraud20050107.asp Fraudulent reconstruction tenders and advance fee fraud following natural disasters. Interpol (4/11/2011)

https://www.interpol.int/Public/FinancialCrime/FinancialFraud/DisasterCharityFraud200501.asp Disaster Charity Fraud. Interpol (4/11/2011)

http://www.fbi.gov/news/stories/2005/january/tsunami_scam010505 Tsunami Disaster Relief Fraud Alert! Don't be Scammed. FBI 1/5/2005

http://www.fbi.gov/scams-safety/e-scams/e-scams Haitian Earthquake Relief Fraud Alert. FBI (2/11/2011)

http://www.fbi.gov/birmingham/press-releases/2011/national-disaster-fraud-hotline-available-to-report-storm-related-fraud National Disaster Fraud Hotline Available to Report Storm-Related Fraud. FBI U.S. Attorney's Office May 10, 2011 (4/11/2011)

https://www.interpol.int/Public/FinancialCrime/FinancialFraud/DisasterCharityFraud200501.asp Financial Crime Disaster Charity Fraud. Interpol (4/11/2011)

http://www.ic3.gov/media/2010/100118.aspx National Center for Disaster Fraud to Coordinate Haitian Fraud Complaints. U.S. Department of Justice Federal Bureau of Investigation18/1/2010 (4/11/2011)

http://www.online.donation.events.org/ Example of middle service provider (4/11/2011)

http://www.donate.net/html2/wwwroot/about_us.asp Donate.net Example of complex middle service provider (4/11/2011)

http://www.oecd.org/dataoecd/30/20/42232037.pdf Report On Abuse Of Charities For Money-Laundering And Tax Evasion. Organisation For Economic Co-Operation And Development Centre For Tax Policy And Administration (22/10/2011)

http://www.hmrc.gov.uk/mlr/news/pakistan-floods-disaster.htm Pakistan floods disaster - guidance on transmitting money. HM Revenue & Customs (29/10/2011)

http://www.justice.gov/usao/mow/news2011/disaster_fraud_tips.pdf Tips for Identifying or Avoiding Becoming a Victim of Disaster Fraud. FBI (21/10/2011)

www.fatf-gafi.org Financial Action Task Force

http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/DI144-2007-08.pdf Cyprus Securities and Exchange Commission Example list to identify suspicious transactions

http://www.charitycommission.gov.uk/RSS/News/pr_pakistan_scam.aspx Be aware of possible Pakistan appeal scams, says Charity Commission. Charity Commission (29/10/2011)

*in the order of occurance in the text