Between Awareness and Ability: Consumers and Financial Identity Theft

Nicole S. van der MEULEN
The Centre of Expertise (HEC), the Hague

Abstract: The role consumers play in the facilitation of financial identity theft is an important topic of discussion. Academics often side with consumers and recognize them as victims rather than facilitators. Others, both in the public and the private sector, believe consumers play a more prominent role in the facilitation of financial identity theft. This is particularly apparent through the popularity of public awareness campaigns. Neither of these accounts manages to reflect the complexity of the overall picture. The following article demonstrates how the role consumers play is continuously changing as a result of the evolution of methods used by perpetrators of identity theft. This evolution requires a different response from both the public and the private sector as consumers lose more control over their potential indirect facilitation of financial identity theft.

Key words: Financial identity theft, consumers, information security, public awareness campaigns.

On July 27, 2009, the Ministry of Justice of the Netherlands launched a large public awareness campaign to prevent citizens from falling victim to cybercrime. [1] During five weeks, the campaign which features a fictional character 'Sandra', was seen on television and heard on the radio. In the commercial used for the campaign, Sandra reveals all. Her bank account number, pin code, log-in name, and video tapes of her holiday at the beach are made public. Sandra herself watches and listens as people gather on the street to witness the publication of all her information. She appears flabbergasted. She is the perfect depiction of the unaware and naïve citizen. Security on the Internet, the campaign claims, is in your hands. [2]

The continued proliferation of public awareness campaigns which emphasize the potential for and the ability of consumers to protect

[1] See http://www.nederlandveilig.nl/veiliginternetten/.

[2] In Dutch the slogan is: "*veilig internetten heb je zelf in de hand*."

themselves, against cybercrime in general and financial identity theft[3] in particular, receives both support (CATE, 2001; MILNE, 2003) and resistance (SOLOVE, 2003; HOOFNAGLE, 2005). As a result, there is an ongoing discussion which focuses on the degree to which consumers maintain both the ability and responsibility to 'prevent', or at least reduce the risk of financial identity theft. In particular, SOLOVE (2003) states how even if individuals did take all steps advised to them, significant risk reduction still fails to occur. This lack of significant risk reduction is due to the actions of both the public and the private sector, which play a more prominent role in the facilitation of financial identity theft, according to SOLOVE. In the overall problem, consumers are victims rather than facilitators. Their share in the enablement of the problem is minimal, if existent at all.

Certain sources even consider the emphasis on individual responsibility a mere political strategy to divert the attention away from the 'actual' facilitators (WHITSON & HAGGERTY, 2008). A similar sentiment is echoed by MARRON (2008: 29) when she states: "[t]he problem becomes pitched not as one of systemic institutional culpability, but as lack of awareness on the part of individuals." According to STONE (1989) stories of 'inadvertent cause' are common in social policy. Individuals 'cause' many problems such as poverty, malnutrition, and disease, because they fail to understand the harmful effects of their willful actions. "Inadvertence here is ignorance;" STONE (1989: 286) writes, and "the consequences are predictable by experts but unappreciated by those taking the actions. These stories are soft (liberal) versions of blaming the victim: if the person with the problem only changed his or her behavior, the problem would not exist." Awareness campaigns, such as the one described above, appear to depict such a story of inadvertent cause. While various authors reject this claim, they do so based on the argument that the role of both the public and the private sector overshadows the impact of consumer actions.

This article aims to shed a different light on the ongoing discussion and accepts an alternative position in an effort to add another dimension to the debate. Rather than rejecting the focus on user education based on the actions of the public and the private sector, this article aims to demonstrate

[3] Financial identity theft for the purposes of this article refers to both account takeover and true name fraud. Account takeover occurs when perpetrators obtain the credentials of an existing account of another individual and use such credentials to drain the account's balance. True name fraud, on the other hand, occurs when perpetrators manage to obtain sufficient personal information about another individual to open a new account or request a new credit card in the name of the other person.

how user education and awareness campaigns fail to address the range of threats faced by consumers, in their role as facilitators of financial identity theft. This failure is important to take into consideration with respect to future policy initiatives set forth in an effort to reduce the risk of financial identity theft. The three categories presented below aim to depict how the evolution of the methods used by perpetrators has theoretically led to a crucial expansion of ways to take advantage of consumers, and how the consumer's ability to actively control the facilitation process is slowly, but surely, diminishing.

■ The others

Before delving into the manners through which consumers can potentially facilitate the first stage of financial identity theft, the comprehensive character of the argument developed within this contribution requires a brief reflection on the potential facilitation of other actors. [4] As indicated in the introduction, the role played by other actors, such as government agencies, financial service providers, data brokers, etc., is often used to illustrate how restricted the influence of consumers is on the prevention of financial identity theft (See SOLOVE, 2003; HOOFNAGLE, 2005; HOOFNAGLE, 2009). This is the case for two reasons. First of all, the only influence consumers may exert with respect to the facilitation of financial identity theft is in relation to the first stage, where perpetrators acquire the personal information needed to either commit true name fraud or account take over. The second stage, where perpetrators abuse the previously obtained personal information, is at the discretion of the public and the private sector, through the means of authentication implemented for e-government and e-commerce or e-banking transactions, respectively. Consumers may mitigate the damage through being more alert and keeping a close watch on account activity and credit reports; but this can only mitigate, not prevent or reduce risks.

The second reason for the restricted influence of consumers is the extensive information collection and storage exercised by the public and the private sector. Over the years, this massive collection and storage of personal information has drawn significant attention as a result of the

[4] This article is an excerpt of the author's doctoral dissertation *Fertile Grounds: The Facilitation of Financial Identity Theft in the United States and the Netherlands*, where 'the others' receive a far more extensive analysis with respect to their potential facilitation of financial identity theft.

publicity afforded to several major data security breaches. To what extent data security breaches actually contribute to financial identity theft is a challenging question to answer (See GOVERNMENT ACCOUNTABILITY OFFICE, 2007). Whilst it is difficult to determine where the information misused for financial identity theft purposes originates, certain breaches have been directly connected to incidents of financial identity theft. A prime example is Choicepoint, a large data broker in the United States, which suffered a highly publicized data security breach several years ago (see SULLIVAN, 2005). According to the official complaint issued by the Federal Trade Commission (FTC), the Choicepoint data breach led to at least 800 cases of identity theft. [5] Due to the pioneering data breach notification legislation in California, Choicepoint was obligated to notify consumers of the breach. In total, Choicepoint notified 163,000 consumers, according to the FTC. The sheer size of such data security breaches certainly appears to trump the potential for facilitation of individual consumers with respect to financial identity theft. And since these data security breaches are widespread [6] in both the public and the private sector, the impact of consumer actions appears limited. This limitation, however, can also be illustrated and extended through a different venue, which is the primary contribution this article aims to make.

■ 'Voluntary' facilitation

The term 'voluntary' is problematic because its usage within the current context can lead to misguided interpretations. Voluntary facilitation here mainly refers to information dispersion which is unprompted by the perpetrator. The term is mainly used to indicate the distinction between the current and the subsequent categories of facilitation, and does not carry any normative implications. The voluntary exposure of consumers' personal information can facilitate the first stage of financial identity theft. Perpetrators have developed several methods to potentially take advantage of such exposure. Among the most infamous methods is dumpster diving. Basically, unsuspecting consumers toss out various documents containing sensitive personal information. Perpetrators become aware of this and start

[5] *United States of America* v. *ChoicePoint* (2006). Supplemental stipulated judgment and order for permanent injunction and monetary relief: 4.

[6] The Privacy Rights Clearinghouse and the Identity Theft Resource Center, among others, maintain records of reported data security breaches in the United States.

rummaging through garbage cans in search of these documents. Many times, one document does not contain all of the necessary information, but perpetrators combine different pieces of garbage to complete the picture. Several years ago, receipts still contained valuable information including the full credit card and account number, which proved to be an attractive source for perpetrators. Overall, consumers would unwittingly and voluntarily present perpetrators with their valuable personal information. Dumpster diving, as a method, took advantage of the voluntary and active participation of consumers.

More recently, other potential opportunities for perpetrators of financial identity theft have evolved through consumers who dispose of old computers, which contain, yet again, valuable personal information. Even if consumers believe they have cleared their hard drive of all data, they are often wrong. The data erased on their hard drive can easily be recovered by perpetrators. Various authors acknowledge this vulnerability (VALLI, 2004; BENNISON & LASHER, 2004).

As the more 'physical' types of voluntary consumer facilitation fizzle out, the focus turns to the digital arena. Much attention has been devoted to the presence of individuals on social networking sites, and in particular the information shared on such fora. In theory, social networking sites such as Facebook, MySpace, and Twitter provide the ideal outlet to let everyone know nearly everything about oneself. Much research aims to demonstrate how users of social networking sites perceive privacy and potential privacy risks associated with their presence on such sites (see for example GROSS & ACQUISTI, 2005; JONES & SOLTREN, 2005; DEBATIN *et al*., 2009). Such research generally provides conclusions which illustrate a lack of concern with the provision of personal information on the part of consumers and the ability for a wide public to view such information (see, in particular, GROSS & ACQUISTI 2005). This willingness to share personal information surpasses the area of social networking sites. Through an experiment, GROSSKLAGS & ACQUISTI (2007: 14) demonstrate how "[...] most subjects happily accepted to sell their personal information even for just 25 cents, and virtually all subjects waived the option to shield their information."

BILGE *et al*. (2009) furthermore demonstrate how perpetrators of financial identity theft can access personal information maintained on profiles of users. This occurs through, for example, profile cloning where perpetrators 'clone' the profiles of authentic users and request to be added as a friend. Perpetrators send these requests to the social network of the 'cloned' individual rather than to random strangers. From the experiment of profile cloning, BILGE *et al*. (2009: 557) conclude how:

> "[...] the friendship acceptance rate for the forged profiles was over 60% for all the forged accounts (in one case, being as high as 90%). The acceptance rate from unknown users was constantly below 30% [...] These results confirm that by forging profiles, an attacker can achieve a higher degree of success in establishing contacts with honest users than when using fictitious accounts."

The outcomes of the various research projects appear to be relevant since identity theft is mentioned on a regular basis as a potential risk associated with social networking site activity (see DONATH & BOYD, 2004; GROSS & ACQUISTI, 2005; STUTZMAN, 2006; BOYD & ELLISON, 2008; IBRAHIM, 2008; STRATER & LIPFORD, 2008). Whether such a risk is viable depends largely on the type of personal information provided by users of the sites.

Despite the lack of apparent empirical evidence demonstrating misuse of personal information obtained from social networking sites for the purposes of financial identity theft, much discussion focuses on the distribution of responsibility with respect to security aspects of such sites. Based on the results of their experimental research, BILGE *et al*. provide suggestions for improvements of security on social networking sites. In their suggestions, the authors acknowledge how users continue to be the weakest link but improved security requires the involvement of the social networking sites. BILGE *et al*. provide the recommendation for social networking sites to provide more information on the authenticity of the friend request and the user who initiated the request.

Whereas BILGE *et al*. direct suggestions toward the sites as opposed to the users, GRIMMELMAN (2008) focuses on the users. GRIMMELMAN (2008: 1140) states how:

> "It's temptingly easy to pin the blame for these problems entirely on Facebook. Easy - but wrong. Facebook isn't a privacy carjacker, forcing its victims into compromising situations. It's a carmaker, offering its users a flexible, valuable, socially compelling tool. Its users are the ones ghost riding the privacy whip, dancing around on the roof as they expose their personal information to the world."

Grimmelman therefore argues in favor of an educational approach which specifically targets users of social networking sites in an effort to help understand the risks associated with the exposure of their personal information.

Even so, the usage and retention of personal information provided to Facebook by Facebook is a topic of heated discussion. Facebook 'shares' information received from users with third parties. This occurs when users install Facebook applications or gadgets. FELT and EVANS (n.d.) write how:

> "[w]hen Jane installs a Facebook application, the application is given the ability to see anything that Jane can see. This means that the application can request information about Jane, her friends, and her fellow network members. The owner of the application is free to collect, look at, and potentially misuse this information."

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) (2008) filed a complaint against Facebook in 2008 alleging 22 separate violations of Canadian privacy law. These violations included Facebook's failure to inform users of how Facebook discloses their personal information to third parties for advertising and other profit-making activities, and Facebook's failure to obtain permission from its users for such uses and disclosures of the personal information of its members (CIPPIC 2008). The user outrage did not occur until the following year when Facebook made changes to its terms of service which led to increased media attention about the practices of the social networking site (see STELTER, 2009). Facebook changed the terms of service and deleted a provision which allowed members to remove their content at any time. Moreover, the new language added to the terms of service stated how Facebook would retain the content and licenses of users even after they terminated their accounts (STELTER, 2009).

The importance of the current dispute over Facebook and its treatment of the information provided by its members is the distribution of responsibility with respect to the 'exposure' of personal information. The line between consumer as opposed to business facilitation becomes blurry and this in turn also influences the judgment about the 'facilitator.' For if perpetrators obtain the information from a third party which said third party obtained from a Facebook profile page, who facilitates? This is an important argument in particular because consumer awareness primarily focuses on this type of consumer facilitation, the voluntary information dispersion. Even so, important to note is how the potential connection between personal information exposure on social networking sites and the facilitation of financial identity theft remains largely drawn on theoretical risks rather than empirical evidence. Still the information available on social networking sites, such as date of birth, full name, affiliations can provide indirect assistance to potentially commit financial identity theft. From the 'old fashioned' method of dumpster diving to the more innovative method of perusing social networking sites, the argument goes that perpetrators cleverly take advantage of both the 'carelessness' and the 'cluelessness' of consumers. This is certainly the area over which consumers have a sense of 'control' and an area in which consumer awareness may at least have some success. This category indicates how, especially as consumers become more knowledgeable about the dangers present in contemporary society, there is at least some room for improvement with regard to reducing consumer facilitation. In contrast, the subsequent two categories begin to demonstrate a shift with regard to consumer control and the level of voluntary involvement on the part of consumers.

■ Social engineering

When consumers do not provide the information voluntarily or unprompted, perpetrators themselves have to hunt for it. And they have managed to do so rather well. In contemporary society, phishing has become a well-known concept, especially among those involved in various areas related to digital technology. The underlying principle of phishing, which is gaining personal information through social engineering techniques, is far from new. As DANG (2008: 8) notes:

> "[w]hether it's called social engineering, trickery, confidence tricks, cognitive biases, or scams, the concept of exploiting a person's naivety and trust is as prevalent today as it has been since the dawn of time."

The craft of the con artist has always been present and used for a variety of criminal activities. Before the Internet domination, perpetrators used more traditional means such as calling and ringing doorbells trying to obtain valuable information. Mitnick, one of the most 'infamous social engineers' in the modern era, carefully outlines how con artists used more 'old-fashioned' social engineering techniques, such as calling, to obtain valuable information from businesses. Through the art of persuasion, con artists successfully managed to convince employees of various corporations to surrender pivotal business information, including passwords (MITNICK *et al.* 2002). The ultimate art used by perpetrators is to convince the target, whether a business or a consumer, that they are someone else, someone trustworthy. The Internet provided and continues to provide perpetrators with the ideal platform to update their old techniques and to more efficiently target consumers. The variety of ways perpetrators incorporate social engineering techniques on the Internet is rather impressive, even during the early days. Special Agent RILEY (1998: 7) described how:

> "[o]ne of the most popular things to do to get people to give up their personal information is to offer credit card accounts at a very, very low interest rate, such as 4.9 or 5.9 percent."

Perpetrators developed websites to offer credit card accounts in search of personal information. RILEY (1998: 8) offers another example when she describes how:

> "[i]n addition to the credit card applications themselves, several others of the schemes that are available out there right now include credit rescue operations where pages, again, using very high-quality graphics are made to look legitimate and offer the ability for you to wipe out any credit problems you have simply, again, by providing all of your personal financial information."

Especially during the early days of the Internet, consumer awareness about potential fraud schemes was severely absent. Perpetrators gratefully managed to take advantage of this absence.

The first actual phishing 'attacks' differed greatly from their current counterparts. The term phishing entered the circuit in 1996 when hackers managed to get unsuspecting America On-line (AOL) users to reveal their passwords. With their passwords, the hackers could gain free internet access (RAMASTRY, 2004). Since then, phishing appears to have become an attractive profit making strategy for various perpetrators involved in financial identity theft. In the beginning phishing emails maintained a sense of amateurism, which provided consumers with the opportunity to potentially detect foul play. Emails sent to Dutch consumers, for example, contained errors which automatically carried an air of suspicion. An infamous email sent by perpetrators posing as the Postbank, a former Dutch bank, made the mistake of using the opening *Lieve Postbankklant*, which directly translates into "Dear Postbankclient," except the dear used in the phishing emails is reserved for communication with close friends and loved ones. Furthermore, the email mainly uses the informal "you" (*je*), similar in German *du* and in Spanish *tu* as opposed to the more formal and more appropriate *u*, or in German *Sie* and Spanish *usted*, which is a direct sign that there is something out of the ordinary going on. Despite the apparent errors, the initial attack led some clients to click on the link and as such the bank was forced to replace all usernames, passwords and TAN codes. This also occurred in other European countries. As DIRRO & KOLBERG (2008: 24) note:

> "In the early days, messages were composed in a crude German notation that looked like it was an English or a Russian text translated by Babel Fish. That's probably what happened."

As information on phishing attacks began to grow, perpetrators also expanded and sophisticated their methods. DANTU *et al*. (2008) describe how the nature of phishing attacks changed over time. Whereas initial attacks were passive such as password guessing and eavesdropping, more recent attacks are active through the employment of Trojans, traffic interception, and the adoption of social engineering techniques. The introduction of phishing as a vehicle to commit financial identity theft led to crucial research on consumer behavior and phishing detectability (see, for example, JAKOBSSEN, 2007). Both academic and non-academic researchers aimed to analyze the awareness of consumers with regard to phishing attacks and their ability to recognize phishing emails. DHAMIJA *et al*. (2006) conducted a usability study to determine which phishing strategies proved successful. The best phishing website managed to fool 90% of the participants through its incorporation of padlock in content, Verisign logo and certificate validation seal, and a consumer alert warning.

This is a crucial development with regard to consumer facilitation and the perception held by society about such facilitation. The media, along with policy makers and business professionals, often refer to popular research conducted by, for example, Javelin Strategy & Research. JAVELIN (2005) concluded how consumer awareness of phishing is high. Such a conclusion paints a bit of a deceiving picture of the relationship between phishing awareness and consumer ability. Basically, through proclaiming a high consumer awareness of phishing, Javelin allows the remainder of society to believe consumers can resist the phishing threat. And have the means to do so. This is a potentially misleading conclusion. Awareness itself may be high, but unless consumers realize financial service providers shall only request personal information during the process of a digital transaction, such awareness is worth little in light of the increased sophistication of phishing attacks. As a result, whereas certain rules, such as financial service providers exclusively asking for particular information while in the midst of a transaction, can certainly decrease the likelihood of a successful phishing attack, others which focus on particular indicators cannot compete with the ability of perpetrators of financial identity theft to imitate those same indicators. DANTU *et al*. (2008: 4) acknowledge how:

> "[t]he major factors in any phishing attack are forgery and social engineering. No matter how many authentication techniques we develop phishers always adapt."

Others, however, disagree. BARRETT (Qtd. in Georgia Tech Information Security Center 2009: 8) states how he believes:

> "[...] phishing is a completely preventable crime when you combine technology with education. Our anti-phishing efforts with Yahoo over a 10 month period prevented more than 85 million phishing emails from ever reaching the intended victim. And if we can teach end users some simple rules, it will have a big impact."

DONG *et al*. (2008), on the other hand, reject the value of user education as a means to 'prevent' successful phishing attacks or to solve the problem. Others recognize value in user education, but criticize the ways through which such education is administered (HARLEY & LEE, 2007; MARTIN, 2009). Herein rests perhaps the most promising approach, since, as indicated above, certain simple rules can have a big impact if they focus on the more overarching aspects of digital communication originating from financial service providers.

While phishing remains a popular topic and method for perpetrators of financial identity theft, the increased usage of multiple factor authentication mechanisms [7] obviously diminishes their rate of success. This is since merely obtaining log in information and passwords are insufficient means to access an account, and subsequently complete transactions in an effort to drain the account.

■ Involuntary facilitation

The increased sophistication of phishing proved to be a foreshadowing of a progression into the 'involuntary' state of consumer facilitation. The incorporation of social engineering techniques still heavily relies on the voluntary participation of consumers to surrender their personal information. Such reliance is far from desirable for perpetrators. As a result, perpetrators

[7] For a successful attack on a multiple factor authentication scheme, perpetrators must engage in a man-in-the-browser (MITB) attack, which surpasses merely obtaining the creditentials of the victims. The MITB attack circumvents the two-factor authentication means through placing the perpetrator between the client and the bank. This occurs through the use of Trojan horses. Whereas perpetrators of traditional phishing attacks develop fraudulent websites to obtain the credentials of clients, victims of MITB attacks actually arrive at the legitimate website of their financial service provider. Yet, through interjecting themselves between the client and the bank, perpetrators manage to receive the communication from both sides and divert transactions to different accounts.

managed to develop means to benefit from consumer facilitation without the need of their active participation. While previously introduced methods have not disappeared, the turn to sophisticated methods of involuntary and passive facilitation certainly influences the means, or lack thereof, of consumer control. As LYNCH (2005: 278) notes:

> "[...] recent phishing attacks have become more sophisticated and involve technological devices that may be beyond the ken of even relatively savvy consumers. Some of these attacks, such as those that automatically change a recipient's hostfile, do not even require any action to be taken by the consumer, so she would be hard-pressed to educate herself on how best to protect herself from this type of attack."

The main drive behind involuntary consumer facilitation is the presence of botnets. According to various authors (LEE *et al.* 2007; GRIZZARD *et al.*, 2007; HUNTER, 2008), botnets have become one of the largest security threats in contemporary society. HUNTER (2008: 13) explains how "[i]ndeed one of the reasons for the botnet becoming the number one security threat lies not in the innovation of its method of recruitment or attack, but in its resistance to defence." Other authors echo similar concerns (BRAND *et al.*, 2007). Its other main attractive feature is its speed. Botnets are:

> "[...] networks of infected end-hosts, called bots, that are under the control of a human operator commonly known as botmaster. While botnets recruit vulnerable machines using methods also utilized by other classes of malware […] their defining characteristic is the use of command and control (C&C) channels" (ABU RAJAB *et al.*, 2006: 41).

Through these channels, the botmasters can send out commands to their 'botarmies.' The creation of botarmies is surprisingly easy. IANELLI & HACKWORTH (2007) describe how creating a botnet only requires 'minimal technical skill.' This is predominantly a result of the assistance of the underground community. The community is more than willing to share its vast knowledge through a variety of channels. Seasoned perpetrators, for example, provide training sessions and advice to newcomers through Internet Relay Channels (IRC) (IANELLI & HACKWORTH, 2007). Through the spread of knowledge, seasoned perpetrators can assist in the increasing growth of botnets around the world. The growth leads to a greater challenge for detecting and subsequently taking down botnets.

The introduction of bot software occurred around the start of the millennium (McLAUGHLIN, 2004). Although "Windows internet worms entered the wild in the late 1990s, leading to the automation of malicious code. Bots emerged from this landscape" (DUNHAM & MELNICK, 2008: 1).

Botnets, however, seemed to have gained the most attention during the past few years and have various goals. These fall into three categories, information dispersion, information harvesting and information processing. With regard to financial identity theft, information harvesting and information dispersion are the most relevant goals. GRIZZARD *et al*. (2007: 3) describe how:

> "[…] information dispersion includes sending out spam, creating denial of service attacks, providing false information from illegally controlled sources, etc. The goal of information harvesting includes obtaining identity data, financial data, password data, relationship data (i.e., email addresses of friends), and any other type of data available on the host."

Botmasters create botarmies through the deployment of malware. Perpetrators can manipulate the installation of malware through a variety of channels. They can seduce consumers into downloading an executable file through, for example, a phishing attack or they can send the malware along with another download. More recently, perpetrators have introduced even more undetectable and more involuntary means of installing malware. As PROVOS *et al*. (2008: 1) note:

> "In most cases, a successful exploit results in the automatic installation of a malware binary, also called drive-by-download. The installed malware often enables an adversary to gain remote control over the compromised computer system and can be used to steal sensitive personal information such as banking passwords, to send out spam or to install more malicious executables over time."

Drive-by-downloads are dangerous because detection of such downloads is extremely difficult for consumers. As such these attacks are a significant threat and deserve considerable attention. Through the drive-by-download, perpetrators manage to install malware, which can include keyloggers. These keyloggers function much like cameras and capture all information typed into the computer. This makes the collection of personal information easy and convenient for perpetrators of financial identity theft. Especially, since consumers are most likely unaware of the presence of a keylogger since its installation via the drive-by-download also occurred without the knowledge of the consumer.

The data obtained via keyloggers is subsequently transferred to dropzones. These dropzones are publicly writable directories on an Internet server which serves as an exchange point for keylogger data (HOLZ *et al*., 2008). Important to note, is how:

> "Contrary to conventional wisdom, the malicious pages weren't mostly hosted on the seedier parts of the internet such as adult and gambling websites. While there were a large number of drive-by infections on adult sites, the majority of the malicious data is hosted on sites whose categorisation is more mundane such as finance, home and garden, and business" (POTTER, 2008: 19).

According to SONG *et al*., (2010), drive-by downloads are currently one of the most severe threats for users of the Internet. Moreover, such downloads are presently the number one malware vector (SONG *et al*., 2010).

■ Analysis

What is happening is a shift in various aspects of the potential for consumer facilitation. In previous years, perpetrators appeared to benefit from the 'carelessness' or 'cluelessness' of consumers. Especially those individuals who would toss out important documents without in some way destroying the personal information exposed. Basically, perpetrators could benefit from the unprompted availability of personal information. As financial identity theft, however, moved into the digital realm it appears as though perpetrators smelled the opportunity to hunt for personal information, without running a high risk of getting caught. This allowed them to gain more control over which information they could obtain and from whom.

There is a subsequent movement from voluntary and active to involuntary and passive consumer facilitation. This movement, demonstrated through the continuous evolution of methods used by perpetrators and detected by those trying to counter the problem indicates a diminishing dependability on actual consumer actions. 'Old-fashioned' methods are certainly still in circulation, but the expansion of opportunities allows especially the sophisticated criminals to carry out their operations with the most advanced methods. These perpetrators find an easy 'in' and they can manage to do everything themselves from there on out. Botnets immaculately reflect this current state of affairs. These botnets have become the epitome of involuntary and passive consumer facilitation, especially through the introduction of 'drive-by downloads,' which are according to various sources among the most common methods for spreading malware these days (EGELE *et al*., 2009a).

Whereas with phishing emails, consumers received a prompt to release personal information in an active manner, perpetrators have managed to eliminate this need for active consumer involvement through the introduction of drive-by downloads. The lack of active consumer involvement means consumers may facilitate aspects of financial identity theft without actually having the ability to prevent or control such facilitation. This is a vital aspect to bear in mind with respect to the potential facilitation of financial identity theft, especially in light of countermeasures and the potential for their effectiveness. Certain sources (BRENNER & CLARKE, 2005: 17) appear to neglect the ability factor when they write:

> "We must realize that we are the front line of defense against cybercrime; we must understand that our carelessness could facilitate a successful cyberterrorist or information warfare attack on the critical infrastructures of our society."

This is not about carelessness anymore. Perpetrators have now managed to place their entire operation outside of the reach of consumers, which makes the act of crime repression, let alone prevention, far more challenging. The technological sophistication of current operations requires significant background knowledge which even the savviest consumers often do not posses. They, along with their instruments such as their computers, are used without their knowledge or influence. This movement creates more challenges because old band-aids such as awareness campaigns start to become even less valuable; yet, the consumer remains a primary target of perpetrators of financial identity theft, especially on the electronic superhighway and as such requires attention.

Despite the diminishing amount of consumer control through the evolution in methods used by perpetrators, consumer awareness campaigns remain a popular tool. Consumer education has been a part of the financial identity theft problem since the early days. The United States government incorporated the element of consumer education into its Federal Identity Theft Assumption and Deterrence Act of 1998 through its request for the establishment of a consumer complaint center. This complaint center, which the Federal Trade Commission needed to create, was to dispense consumer education tools in order to make consumers aware and better equipped to combat the increasing threat of financial identity theft. [8] Perpetrators of

[8] See Title 18 USC §5: Centralized Complaint and Consumer Education Service for Victims of Identity Theft which states: "(1) log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief that 1 or more of their means of identification (as defined in section 1028 of title 18, United States Code, as amended by this Act) have been

financial identity theft, after all, thrive on the abundance, availability, and accessibility of personal information in order to carry out their operations. Back then, more than a decade ago, such consumer education appeared crucial due to the lack of awareness about the existence of such a crime. The notion of consumer education as a means to raise awareness is evident in various sectors of society (BRUHN, 1997; WOOD & WAHL, 2006) as is empirical research on their effectiveness, or lack thereof (BROWN, 2000). While certainly consumer education is important in an overall action plan to counter financial identity theft, their role and value should not be overestimated.

■ Alternatives

The ineffective nature of consumer awareness campaigns inevitably begs the question as to a more appropriate type of response. This response is necessary because perpetrators of financial identity theft continue to target consumers in order to carry out their activities. And consumers themselves continue to conduct more and more transactions online through the continuous proliferation of electronic services offered by both the public, through electronic government, and the private sector, through electronic commerce and online banking. The focus itself therefore on the individual as the main driver behind the development of solutions is understandable and important, especially since the individual is often considered the weakest link. The main challenge is to focus on the individual yet bear in mind the individual's 'inability' or rather limited ability to conquer the most advanced threats to information security. A glance at the reduction of other crimes provides limited inspiration. VOLLAARD (2009) provides empirical evidence for the success of government intervention in the Netherlands with respect to high-quality locks and burglary-proof windows. Starting in 1999, the government required all new-built homes to have these high-quality locks and burglary-proof windows. Through this government requirement, the Building Code needed to be adjusted accordingly. Vollaard describes how the change in the Building Code reduced the burglary risk in newly built homes by 50 percent. Through these results, Vollaard considers the government regulation for built-in security an effective means to lower crime

assumed, stolen, or otherwise unlawfully acquired in violation of section 1028 of title 18, United States Code, as amended by this Act." (2) provide informational materials to individuals described in paragraph 1.

and also determines how the regulation maintains considerable social benefits. The government regulation also proved more effective than other measures taken to lower levels of crime such as altering the preferences of potential offenders or the preferences of victims for precaution (VOLLAARD, 2009). Such built-in security may also be an attractive option for the threats described in this article. EGELE *et al*. (2009b: 11) elaborate on such a solution when they "[...] propose to have defense mechanisms built into the browser itself to mitigate the threats that arise from drive-by download attacks." Such built-in security takes into consideration the limited ability of consumers to protect themselves against the most recent threats in the digital world. Perhaps the success in the physical world can be transferred to the digital realm.

Even so, as became obvious through the brief reflection on the others above, a comprehensive response to the problem of financial identity theft requires additional measures in an effort to curb the facilitation of the phenomenon. This is precisely because the consumer share only represents a fraction of the problem. One (promising) suggestion, for example, which focuses on the others, is a strict liability approach for financial service providers as a means to develop stronger and direct incentives (HOOFNAGLE, 2009). This focus on incentives is crucial, as Hoofnagle notes, especially since they are "the core of the identity theft problem" (HOOFNAGLE, 2009). The focus on incentives has demonstrated its significance through the introduction of data security breach notification legislation around the world, which in part aims to increase the incentives for organizations to improve their information security practices in an effort to reduce the risk of financial identity theft. Since the facilitation of financial identity theft occurs through the actions of multiple societal actors, its response must also take into consideration these same actors as well as their actions. This article and the suggestion for build-in security are therefore a piece of the puzzle.

■ Conclusion

The introduction of this article provided a brief portrayal of the complexity surrounding the role of *consumers* in the facilitation of financial identity theft. Whereas the threats in the virtual world evolve, the overall discussion about consumers remains focused on the more traditional methods of perpetrators, which means the threat of involuntary facilitation remains largely out of sight.

Those directly involved in the area of information security are acutely aware of the most recent trends and threats, as their valuable research demonstrates. Those in the area of public policy nevertheless appear to have failed to catch on to the changes; at least, if the emphasis on public awareness campaigns geared toward consumers is a reliable indicator. As the above description and analysis demonstrate, the facilitation of consumers is multi-faceted and continuously evolving as perpetrators discover new opportunities. The current trend appears to be a move away from a stage of active and voluntary facilitation to a stage of passive and involuntary facilitation. Through the introduction of botnets and drive-by downloads, perpetrators manage to take advantage of consumers in a largely unnoticeable manner. This shift means that the potential facilitation of consumers is threatening because they might be largely incapable of stopping it, because between *awareness* and *ability* remains a sizeable gap which continues to grow as methods evolve.

References

ABU RAJAB, M., ZARFOSS, J., MONROSE, F. & A. TERZIS (2006): "A Multifaceted Approach to Understanding the Botnet Phenomenon", *Proceedings of ACM SIGCOMM/USENIX Internet Measurement (IMC)*: 41-52.

BENNISON, P.F. & J.P. LASHER (2004): "Data Security Issues Relating to End of Life Equipment", *Proceedings of the 2004 IEEE International Symposium on Electronics and the Environment*.

BILGE, L., STRUFE, T. BALZAROTTI, D. & E. KIRDA (2009): "All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks", Paper presented at the *18th International World Wide Web Conference*. Available at: http://www.csd.uoc.gr/~hy558/papers/p551.pdf (last accessed July 14, 2010).

BRAND, M., CHAMPION, A. & D. CHAN (2007): "Combating the Botnet Scourge. Unpublished Manuscript".
http://www.cse.ohiostate.edu/~champion/research/Combating_the_Botnet_Scourge.pdf (last accessed July 14, 2010).

BRENNER, S.W. & L.L. CLARKE (2005): Distributed Security: A New Model of Law Enforcement. *SSRN Accepted Papers Series.*

BRUHN, C.M. (1997): "Consumer Concerns: Motivating to Action", *Emerging Infectious Diseases*, Vol. 3 (4): 511-515.

Canadian Internet Policy and Public Interest Clinic (CIPPIC) (2008): "CIPPIC files privacy complaint against Facebook", Press release, May 30, 2008.
http://www.cippic.ca/uploads/NewsRelease_30May08.pdf (last accessed July 13, 2010).

CATE, F.H. (2001): "The Privacy Paradox", *76th Annual Winter Newspaper Institute North Carolina Press Association*.

DANG, H. (2008): "The Origins of Social Engineering", *McAfee Security Journal*: 4-8.

DANTU, R., PALLA, S. & J. CANGUSSU (2008): "Classification of Phishers", *Journal of Homeland Security and Emergency Management*, Vol. 5 (1): 1-14.

DAVID, F.M., CHAN, E.M., CARLYLE, J.C. & R.H. CAMPBELL (2008): "Cloaker: Hardware Supported Rootkit Concealment", *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA: 296-310.

DEBATIN, B., LOVEJOY, J.P., HORN A-K. & B.N. HUGHES (2009): "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", *journal of computer-mediated communication*, Vol. 15 (1): 83-108.

DHAMIJA, R., TYGAR, J.D. & M. HEARST (2006): "Why Phishing Works", *Proceedings of the Conference on Human Factors in Computing Systems*: 1-10.

DIRRO, T. & D. KOLBERG (2008): "Germany: Malware learns the language", *Sage*: 22-27.

DONATH, J. & D. BOYD (2004): "Public displays of connection", *BT Technology Journal*, 22: 71-82.

DONG, X., CLARK, J.A. & J. JACOB (2008): "Modelling User-Phishing Interaction", *2008 Conference on Human System Interactions*: 627-632.

DUNHAM, K. & J. MELNICK (2008): *Malicious Bots: An Inside Look*, Auerbach Publications.

EGELE, M., WURZINGER, P., KRUEGEL, C. & E. KIRDA (2009a): "Defending Browsers against Drive-by Downloads: Mitigating Heap-spraying Code Injection Attacks", *Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer: 1-19.

EGELE, M., KRUEGEL, C. & E. KIRDA (2009b): "Mitigating Drive-by Download Attacks: Challenges and Open Problems", unpublished manuscript.
https://www.iseclab.org/papers/inetsec09.pdf (last accessed July 14, 2010).

FELT, A. & D. EVANS (n.d.): "Privacy Protection for Social Networking APIs".
http://www.cs.virginia.edu/felt/privacy/ (last accessed July 13, 2010).

FREDRIKSON, M., MARTIGNONI, L., STINSON, E. & S. J.J. MITCHELL (2008): "A layered architecture for detecting malicious behaviors", paper presented at the *11th International Symposium on Recent Advances in Intrusion Detection (RAID 2008)*.

Georgia Tech Information Security Center, (2009): *Emerging Cyber Threats Report 2009*. http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf (last accessed July 14, 2010).

GOLD, S. (2009): "A Newsworthy Year", *Infosecurity*, Vol. 6: 24-28.

GOVERNMENT ACCOUNTABILITY OFFICE (2007): *Personal Information: Data Breaches are Frequent but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*.

GRIMMELMAN, J. (2009): "Saving Facebook", *Iowa Law Review*, Vol. 94: 1137-1206.

GRIZZARD, J.B., SHARMA, V., NUNNERY, C. & B.B. KANG (2007): "Peer-to-Peer botnets: Overview and Case Study", Paper presented at *Usenix Hotbots 2007*.

GROSS, R. & A. ACQUISTI (2005): "Information Revelation and Privacy in Online Social Networks. (The Facebook Case)", pre-proceedings version *ACM Workshop on Privacy in the Electronic Society* (WPES).
http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf
(last accessed July 14, 2010).

GROSSKLAGS, J. & A. ACQUISTI (2007): "When 25 cents is too much: An Experiment on Willingness-To-Sell And Willingness-To-Protect Personal Information", *Workshop on the Economics of Information Security (WEIS*).

HARLEY, D. & A. LEE (2007): "Phish Phodder: is User Education Helping or Hindering?", *17th Virus Bulletin and Conference Proceedings*.

HOLZ, T., ENGELBERTH, M. & F. FREILING (2008): "Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones".
https://www.fehcom.net/fh-frankfurt/vorlesungen/2008_WS/itsec/material/impersonation-attacks-TR.pdf (last accessed July 14, 2010).

HOOFNAGLE, C.J. (2005): "Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors", *in* A. Chander, L. Gelman, M.J. Radin (Eds), *Securing Privacy in the Internet Age*, Stanford, CA: Stanford University Press.

HOOFNAGLE, C.J. (2009): "Internalizing Identity Theft", *UCLA Journal of Law & Technology*, Vol. 13 (2): 1-36.

HUNTER, P. (2008): "PayPal, FBI and others wage war on Botnet armies. Can they succeed?", *Computer Fraud & Security*, Vol. 2008: 13-15.

IANELLI, N. & A. HACKWORTH (2007): "Botnets as a Vehicle for Online Crime", *The International Journal of Forensic Computer Science*: 19-39.

IBRAHIM, Y. (2008): 'The New Risk Communities: Social Networking Sites and Risk', *MCP* 4 (2): 245-252.

JAKOBSSON, M. (2007): "The Human Factor in Phishing", *Privacy & Security of Consumer Information*: 1-19.

Javelin Strategy & Research (2005): "'Phishing: Consumer Behavior and Awareness", Syndicated Report Brochure.

JONES, H. & J.H. SOLTREN (2005): "Facebook: Threats to Privacy", unpublished manuscript.
http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05papers/facebook.pdf
(last accessed July 14, 2010).

LEE, W., WANG, C. & D. DAGON (2007): *Botnet Detection: Countering the Largest Security Threat*, Springer Verlag.

LYNCH, J. (2005): "Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks", *Berkeley Technology Law Journal*, Vol. 20: 259-300.

MARRON, D. (2008): " 'Alter Reality' Governing the Risk of Identity Theft", *British Journal of Crime and Criminology*, Vol. 48 (1): 20-38.

MARTIN, T. (2009): "Phishing for Answers: Factors Influencing a Participant's Ability to Categorize Email", unpublished manuscript. projects.csail.mit.edu.

McLAUGHLIN, L. (2004): "Bot Software Spreads, Causes New Worries", *IEEE Distributed Systems Online*, Vol. 5 (6): 1-5.

MILNE, G.R. (2003): "How Well Do Consumers Protect Themselves?", *Journal of Consumer Affairs*, Vol. 37 (2): 388-402.

MITNICK, K., SIMON, W. & S. WOZNIAK (2002): *The art of deception: controlling the human element of security*, John Wiley & Sons.

OLLMANN, G. (2008): "The evolution of commercial malware development kits and colour-by-numbers custom malware", *Computer Fraud & Security*, Vol. 28: 4-7.

POTTER, B. (2008): How bad is it?, *Network Security*, Vol. 2008: 18-20.

PROVOS, N., MCNAMEE, D., MAVROMMATIS, P., WANG, K. & N. MODADUGU (2008): "The Ghost In The Browser Analysis of Web-Based Malware".
http://www.usenix.org/event/hotbots07/tech/full_papers/provos/provos.pdf
(last accessed July 14, 2010).

RAMASASTRY, A. (2004): "Hooking Phishermen".
http://www.cnn.com/2004/LAW/08/16/ramasastry.phishing (last accessed July 14, 2010).

RILEY, M. (1998): "Statement to the U.S. Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary", *The Identity Theft and Assumption Deterrence Act*, Hearing, May 20, 1998 (Serial 105-779).

SOLOVE, D.J. (2003): "Identity Theft and the Architecture of Vulnerability", *Hastings Law Journal*, Vol. 54: 1227-1273.

SONG, C., ZHUGE, J., HAN, X. & Z. YE (2010): "Preventing Drive-by Download via Inter-Module Communication Monitoring", *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*: 124-134.

STELTER, B. (2009): "Facebook's Users Ask Who Owns Information", *New York Times*, February 16, 2009.

STONE, D.A. (1989): "Causal Stories and the Formation of Policy Agendas", *Political Science Quarterly*, Vol. 104 (2): 281-300.

STRATER, K. & H. LIPFORD (2008): "Strategies and struggles with privacy in an online social networking community", in *Proceedings of British Computer Society Conference on Human-Computer Interaction*.

STUTZMAN, F. (2006): "An evaluation of identity-sharing behavior in social network communities", Paper presented at the iDMAa and IMS Code Conference, Oxford, Ohio.

SULLIVAN, B. (2005): *Database giant gives access to fake firms: ChoicePoint warns more than 30,000 they may be at risk*. http://www.msnbc.msn.com/id/6969799/ (last accessed July 13, 2010).

VALLI, C. (2004): "Throwing out the enterprise with the hard disk", *2nd Australian Computer, Networks & Information Forensics Conference*, School of Computer and Information Science, Edith Cowan University, Perth, Western Australia: 124-129.

VOLLAARD, B. (2009): "Does regulation of built-in security reduce crime? Evidence from a regression discontinuity approach", paper presented at the *1st Bonn/Paris Workshop on Law and Economics*, September 25-26.

WHITSON, J.R. & K.D. Haggerty (2008): "Identity theft and the care of the virtual self", *Economy and Society*, Vol. 37 (4): 572-594.

WOOD, A.L. & O.F. WAHL (2006): "Evaluating the Effectiveness of a Consumer-Provided Mental Health Recovery Education Presentation", *Psychiatric Rehabilitation Journal*, Vol. 30 (1): 46-53.