Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comment

You've been warned: Consumer liability in Internet banking fraud

Nicole S. van der Meulen [1]

VU University Amsterdam, Faculty of Law, Department of Transnational Legal Studies, The Netherlands

Keywords:
Internet banking
Banking fraud
Online crime
Hacking attacks
Online banking security
Consumer liability

ABSTRACT

This contribution provides a critical analysis of the treatment of consumer liability in cases of Internet banking fraud. Whereas generally banks refund the financial losses associated with Internet banking fraud to the individual victim, exceptions do occur, at least in certain EU jurisdictions. These, however, are rarely spoken about, but do indicate a number of (legal) problems. The main problems are lack of clarity and lack of consistency as to when a consumer can be held liable. These problems also maintain potential negative consequences such as increase in perceived risk, loss of trust and demands for better security, which may be suboptimal from an economical perspective. This article concludes by reflecting on the potential benefits of the introduction of zero liability as an alternative.

1. Introduction

Internet banking fraud is among the most lucrative types of cybercrime in contemporary society. Assessments of financial damages are difficult to come by, especially since financial service providers demonstrate a considerable dislike for transparency on the issue. Even when they do offer such transparency, questions about the reliability of such figures remain. Measurements of any type of online crime are problematic in general (Anderson et al., 2012). There is, however, little doubt among those involved that the problem as a whole is on the rise (see for example Gostev, 2012). Especially the continuously rising number of (successful) phishing attacks is a reliable indicator (APWG, 2013). The growth is mainly due to the evolution of methods used by perpetrators to carry out their attacks (van der Meulen, 2011). The increased sophistication of attacks has complicated prevention and detection efforts, which in turn has allowed their success to proliferate. This has understandably increased the financial burden on both financial service providers as well as consumers. The latter, in particular, are running an increased legal risk of being exposed to financial losses. Yet, this topic is rarely touched upon in academic discussions. The general assumption is that, as Florencio and Herley (2012, p. 63) state, "consumers are not held liable for emptied accounts." This assumption is largely based on the regulatory framework in the United States (through US Regulation E) and the European Union (through EU directive 2007/64/EC), which limits consumer liability to $50 and 150 Euros respectively. Even so, exceptions do occur, especially in the European Union and more particular in the Netherlands. This comment focuses on those rarely discussed exceptions in an effort to lay bare some of the problems with the present manner of dealing with victims who fail to receive a refund after perpetrators have managed to drain their accounts through fraudulent transactions.

[1] Nicole S. van der Meulen is presently working as Assistant Professor at the VU University Amsterdam, Faculty of Law, Department of Transnational Legal Studies. Previously, she worked as an information security advisor for the Dutch government and she holds a PhD in Law from Tilburg University.

0267-3649/$ – see front matter © 2013 Nicole S. van der Meulen. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2013.09.007

The paper also discusses the available cases which have been presented in the media, and in case law, where the consumer found herself liable for the losses incurred as a result of Internet banking fraud. Based on these cases, the associated problems will be discussed such as lack of clarity and lack of consistency. In the subsequent section, the article reviews some potential negative consequences of holding consumers liable, especially under unclear and inconsistent circumstances. The final part of the article reflects on the benefits of zero liability as a potential 'solution' to the problem.

2. Liability

In general, as noted in the introduction, the common conception is that banks refund the financial losses of victims of Internet banking fraud. Some even consider banks as the victims since they suffer the financial penalty of the incidents. In the Netherlands, the practice of Dutch banks has in principle always been to refund the financial losses of victims of Internet banking fraud. This decision is based on the EU Directive 2007/64/EC on payment services in the internal market, specifically article 61, which limits consumer liability to 150 Euros. However, as stated in article 61, "*[t]he payer shall bear all the losses relating to any unauthorised payment transactions if he incurred them by acting fraudulently or by failing to fulfil one or more of his obligations under Article 56 with intent or gross negligence.*" The obligations listed in article 56 are:

> *(a) to use the payment instrument in accordance with the terms governing the issue and use of the payment instrument; and*
>
> *(b) to notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of loss, theft or misappropriation of the payment instrument or of its unauthorised use.*

Generally, the provisions of the Payment Services Directive led banks to refund in all cases. Consequently, the liability front remained quiet. Even the rising number of cases and lost euros did not alter that state of tranquillity. This was until a television programme in the Netherlands, *Kassa!*, focused on consumer affairs, provided a platform for victims of Internet banking fraud who had not received a refund of their stolen funds. The show devoted considerable attention to the first hand stories of victims who fell into the small category of victims whom did not receive their refund. Through showcasing these incidents, *Kassa!* managed to expose a number of challenges associated with the decision making process of the banks in question.

Presently, banks expect more from consumers. After years of awareness campaigns, they count on a certain level of awareness on the side of the consumer. This expectation might also be used as a vehicle to transfer the liability from the side of the bank to the side of the consumer. This leads to the question: to what extent can consumers be held liable for the financial losses of Internet banking fraud? To answer this question, we have to at least determine the issue of causality and reasonableness. The latter concerns the issue whether the victim has acted negligently, which is a challenging issue in light of Internet banking fraud. Banks have always retained the right to refuse refunding victims, in cases of gross negligence. Yet, what exactly entails gross negligence is quite ambiguous since it lacks a clear definition in the present context. As Gijs Boudewijn from the Dutch Banking Association confirms: 'The terms "careless" and "negligent" differ per case, per client and per bank.' This leads to the two main challenges associated with the present state of affairs: lack of clarity and lack of consistency.

2.1. *Lack of clarity and consistency*

The lack of clarity about the qualification of gross negligence and care is particularly problematic since consumers lack a framework they can rely on. Since the terms are open to interpretation, decisions made by different banks can even be conflicting despite a similar set of circumstances. The lack of clarity can lead to a lack of consistency, which makes the decision making process vulnerable to arbitrary decisions that can subsequently be justified through the fluidity of the terms. The lack of transparency often offered by banks about the decision making process in individual cases also fails to illuminate the situation. Especially since banks generally refuse to elaborate on individual cases.

The lack of consistency as a result of the lack of clarity became evident through the following cases. In the episode of *Kassa!* on September 15, two victims received the opportunity to tell their story. The first victim, a client of the ABN Amro bank, received a phishing email. After having opened the email, she received a phone call from 'Vanessa' who claimed to be a banking representative from the ABN Amro. A second victim, a client of the Rabobank, received the same email and phone call. But he spoke to 'Kimberly.' In both telephone conversations, the fraudsters referred to the email they sent.[2] They claimed how due to the phishing email, the accounts of the clients had to be checked and verified for potential 'errors.' To carry out this verification, the clients had to provide the banking employees, or rather the fraudsters, with their e.identifier or random reader codes. By providing these codes, the fraudsters managed to drain the accounts of the victims. They had already obtained the victims' credentials through the phishing emails and with the randomly generated codes they could also carry out the necessary transactions. Both victims found themselves with empty accounts.

The subsequent decisions made by the banks demonstrate the potential arbitrariness. The ABN Amro decides to refund its client, whereas the Rabobank refuses to do so. The Rabobank considers the provision of random reader codes to another person as negligent behaviour, even if clients believe they are communicating with the bank. To support and justify this decision, the Rabobank describes how it posted a warning on the Internet banking screen which specifically warned clients for this type of attack. According to the Rabobank,

[2] The use of the telephone to carry out internet banking fraud also occurs in other countries. The UK Cards Association (2013), for example, describes: "Evidence shows that online banking customers are also being tricked into divulging their login details, passwords and other personal data over the phone to someone they believe is from their bank but is actually a fraudster."