Litigating Cases Involving Hackers Accessing Online Banking Accounts

By: Brendan Collins, Esquire
August 14, 2018

In the age of internet banking, hackers accessing online banking accounts is a widespread problem. One common fraud scheme involves obtaining a business's bank account login information and then replacing intended beneficiary account numbers with account numbers belonging to the hacker or his or her accomplice. The account numbers could be swapped on scheduled outgoing payments or templates for frequently paid vendors. Whether the login information is obtained through a "phishing" attack or malware, unauthorized bank account access can cause the loss of hundreds of thousands or even millions of dollars for which banks often disclaim responsibility.

In the past, parties perpetrating banking fraud often needed to forge payment instructions and/or trick bank employees by phone or in-person. Today, any scammer with unauthorized access to an online bank account can steal funds without needing to forge documents and without even needing to speak to anyone. The fact that a bank offers internet account access for convenience does not allow it to ignore online security risks for its customers. Banks confirm a customer's identity by photographic ID when he or she visits a branch to access an account, and for the same reason, banks need security procedures in place to ensure authorized persons are requesting access to online accounts.

Widespread fraud schemes are one of the primary reasons that commercially reasonable standards in the banking industry require banks to use multi-factor authentication, *i.e.*, to ensure that a single set of user logins cannot enable fraudulent activity. It is also why banks use monitoring and reporting software to detect suspicious and unauthorized activity or compromised user passwords. Banks sometimes fail to utilize such procedures but nonetheless

©GKG Law, P.C. 2018, all rights reserved

deny responsibility for a customer's resulting losses, relying upon disclaimers contained in the bank's boilerplate contracts.

Such contractual defenses may be overcome by relying upon Federal Financial Institutions Examination Council ("FFIEC") Guidance which spell out minimum elements that should be part of a financial institutions security procedures. Courts frequently hold that failure to comply with FFIEC Guidelines reflects that the banking institution has not complied with commercially reasonable banking standards.

GKG would be happy to consult with victims of such banking frauds in order to address whether they have rights arising therefrom. Please contact Brendan Collins or Oliver Krischik at GKG Law if you would like to discuss any issues in this regard. Brendan may be reached by telephone at (202) 342-6793 or by email at bcollins@gkglaw.com. Oliver Krischik may be reached by telephone at (202) 342-5266 or by email at okrischik@gkglaw.com.

©GKG Law, P.C. 2018, all rights reserved