CONSUMER AGREEMENT AUDITS

Reduce Risk Posed by Financial Aggregators and Cyber Attacks

BY TONY MOCH AND ERIK DIDRIKSON

Has your banking organization conducted its annual review of its electronic banking agreements? If you haven't, your organization may want to consider whether revisions are required to your bank's deposit agreements, online banking agreements and other electronic banking services agreements in light of increased activity from financial aggregator websites.

What are financial aggregators?

If you are a bank and you offer online banking, chances are that your site is being accessed by increasingly popular financial aggregators. Products like Mint (owned by Intuit), Banktivity (linked with Apple's OS X operating system) or MoneyDance are free services that offer customers the opportunity to have all of their financial information, ranging from checking accounts and student loan balances to mortgage payments and investment ledgers, all compiled in one easy-to-read display; available anytime, anywhere.

The financial aggregator services operate by asking the user to submit their login information for their online bank accounts. Once the user has provided his or her login information to all of their various online bank accounts, the aggregator services "ping" the customer's bank accounts hosted on the bank's servers to provide the customer with real-time updates to their account balances. The services are ever-increasing in popularity, especially among millennials. The leading service, Mint, boasts over 20 million users.

Why do financial aggregators pose a risk?

The concern with financial aggregator services is the very real potential for cybersecurity breaches. Although it doesn't appear that any aggregator site has been hacked to date, such sites would be a veritable gold mine of a user's entire financial world in just one click. A breach at an aggregator site would in turn provide a hacker with an access point into a bank's online banking network. Moreover, these aggregator sites can have direct cyber infrastructure costs for banks. The constant "pings" to the bank's servers may overload and "crash" the server during peak hours, or at the very least drive up traffic, resulting in higher maintenance fees.

What can you do to reduce your liability?

So how can your bank balance the potential cybersecurity risk from an aggregator with the customer's obvious desire to use such a service? Begin by adjusting your banking agreements to specifically limit the bank's liability in the event of a breach arising from an aggregator site. As part of your bank's annual review and audit of its suite of online banking agreements, account agreements, electronic banking series agreements and other customer agreements, consider including a passage disclaiming liability for any loss stemming from a customer choosing to give their online account information to a third party. Your bank should also consider posting a warning on its online banking portal to the potential security risk that these aggregation sites pose. Finally your bank may want to consider trying to limit aggregator access through physical security measures (e.g., a "two step" verification process).

How can you stay ahead of cyber threats?

As third-party services such as financial aggregator services become more and more popular your organization should continue to review and audit its banking services agreements on a regular basis. Winthrop & Weinstine, P.A. attorneys continually review, advise on and negotiate numerous banking services agreements, including deposit agreements, online banking agreements, third-party vendor agreements and other electronic banking services agreements. Should you wish to discuss your current banking agreements in greater detail, please feel free to contact the Community Banking group at Winthrop & Weinstine, P.A.

ANTON J MOCH
Shareholder
P (612) 604-6671
amoch@winthrop.com
www.winthrop.com/moch

ERIK DIDRIKSON
Associate
P (612) 604-6536
edidrikson@winthrop.com
www.winthrop.com/didrikson

WINTHROP WEINSTINE