DREHER TOMKIES LLP ALERT

FOR CLIENTS AND FRIENDS OF DREHER TOMKIES LLP

November 8, 2016

FINTECH AND FINCEN SARs REPORTING

FinCEN's Advisory to Financial Institutions on Cyber-Events and Cyber Enabled Crime highlights the tension between the FinTech industry and compliance with FinCEN requirements. *See* FinCEN Advisory, Fin-2016-A005 (October 25, 2016). The ease and speed of FinTech services that make such services attractive to customers also make FinTech services attractive to terrorists and criminals.

The FinCEN Advisory states that cybercriminals target the financial system to defraud financial institutions and their customers and to further other illegal activities. Financial institutions can play an important role in protecting the U.S. financial system from these threats. Early this month the Federal Financial Institutions Examination Council issued Frequently Asked Questions regarding its Cybersecurity Assessment Tool that financial institutions may use to evaluate their risks and cybersecurity preparedness. Given this increased attention, FinTech firms and marketplace lenders can expect increased scrutiny from regulators regarding compliance with FinCEN requirements, including those relating to Anti-Money Laundering. While traditional banks have been complying with FinCEN requirements for years in regard to traditional bank products, who is responsible for FinCEN compliance in marketplace lending programs? If the non-bank partner is the first line of defense and maintains the system of record for a bank lending program, is the partner sufficiently aware of the FinCEN requirements?

The Advisory from FinCEN reminds institutions of their obligation to report cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARS). The Advisory states:

> A financial institution is required to report a suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates to $5,000 or more in funds or other assets. If a financial institution knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions, it should be considered part of an attempt to conduct a suspicious transaction or series of transactions. Cyber-events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities.
>
> In determining whether a cyber-event should be reported, a financial institution should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted. Similarly, to determine monetary amounts involved in the transactions or attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event.

The Advisory contains the following examples, each involving no completed transaction:

> Example 1: Through a malware intrusion (a type of cyber-event), cybercriminals gain access to a bank's systems and information. Following its detection, the bank determines the cyber-event put $500,000 of customer funds at risk, based on the systems and/or information targeted by the cyber-event. Accordingly, the bank reasonably suspects the intrusion was in part intended to enable the perpetrators to conduct unauthorized transactions using customers' funds.
>
> The bank must file a SAR because it has reason to suspect the cybercriminals, through the malware-intrusion, intended to conduct or could have conducted unauthorized transactions aggregating or involving at least $5,000 in funds or assets. The bank should include all available information in the SAR relevant to the suspicious activity, including cyber-related information such as a description and signatures of the cyber-event, attack vectors, command-and-control nodes, etc.
>
> Example 2: Through a cyber-event, cybercriminals gain access to a financial institution's systems/networks. The cyber-event exposes sensitive customer information such as account numbers, credit card numbers, balances, limits, scores, histories, online-banking credentials, passwords/PINs, challenge questions and answers, or other similar information useful or necessary to conduct, affect, or facilitate transactions.
>
> By evaluating the cyber-event and the type of information sought by its perpetrators, the financial institution reasonably suspects the cyber-event may have targeted information for the purpose of conducting, facilitating, or affecting transactions aggregating to at least $5,000. For instance, the financial institution could reasonably suspect the cybercriminals intended to steal and sell the exposed sensitive customer information to

Darrell L. Dreher
ddreher@dltlaw.com

Elizabeth L. Anstaett
eanstaett@dltlaw.com

Robin R. De Leo
robin@dreher-la.com

Susan M. Seaman
sseaman@dltlaw.com

Emily C. Cellier
ecellier@dltlaw.com

2750 HUNTINGTON CENTER
41 S. HIGH STREET
COLUMBUS, OHIO 43215
TELEPHONE: (614) 628-8000 FACSIMILE: (614) 628-1600
WWW.DLTLAW.COM

Michael C. Tomkies
mtomkies@dltlaw.com

Charles V. Gall
cgall@dltlaw.com

Judith M. Scheiderer
jscheiderer@dltlaw.com

Susan L. Ostrander
sostrander@dltlaw.com

To see previously sent ALERTS, visit our website at www.dltlaw.com

To decline future ALERTS, please contact us at ALERTS@DLTLAW.COM.
This ALERT has been prepared for informational purposes only. It does not constitute legal advice and does not create an attorney-client relationship.

other criminals for financial exploitation to include unauthorized transactions at the institution. As further described below, the targeted financial institution should file a SAR to report all relevant information, including cyber-related information and information pertaining to any related unauthorized transactions.

To comply with FinCEN anti-money laundering and other legal requirements, FinTech companies and their bank partners need robust Anti-Money Laundering Programs that identify cyber-incidents/attempts as possible reportable events for SARs purposes.

We can assist companies in developing and reviewing their Anti-Money Laundering Programs. ❑

✧ *Elizabeth Anstaett and Mike Tomkies*

© 2016 DREHER TOMKIES LLP