DREHER TOMKIES LLP ALERT

FOR CLIENTS AND FRIENDS OF DREHER TOMKIES LLP

October 19, 2022

NYDFS ENTERS INTO CONSENT ORDER WITH EYEMED FOR DATA BREACH

On October 18, 2022, the New York Department of Financial Services (the "Department") announced that it entered into a consent order with EyeMed Vision Care LLC for alleged violations of New York's Cybersecurity Regulation related to a cybersecurity event. EyeMed is licensed to sell life, accident and health insurance in New York by the Department and subject to oversight by the Department.

In 2017, New York's first-in-the-nation Cybersecurity Regulation became effective. The Cybersecurity Regulation applies to Department regulated entities, which include any person operating under a license, charter or similar authorization under the New York Banking Law, the New York Insurance Law or the New York Financial Services Law. The Cybersecurity Regulation requires such entities to establish a cybersecurity program based on the entities' risk assessment to protect consumer nonpublic information ("NPI").

EyeMed reported a cybersecurity event to the Department on October 9, 2020, as required by the Cybersecurity Regulation. The exact origin of the cybersecurity event is unknown, but believed to be the result of a successful phishing scam email. The cybersecurity event lead to bad actors being able to access emails and attachments containing NPI dating back six years.

Through investigating the cybersecurity event, the Department concluded that EyeMed violated the Cybersecurity Regulation by not limiting user access privileges to information systems that provide access to NPI, by not implementing multi-factor authentication for all users or a reasonable equivalent or more secure access control approved in writing by the chief information security officer and by not having policies and procedures in place for the secure disposal on a periodic basis of any NPI in the mailbox once the NPI was no longer necessary for a legitimate business purpose, among other alleged violations.

Under the consent order with the Department, EyeMed is required to pay a monetary penalty of $4.5 million and implement certain remedial measure to strengthen controls to protect its cybersecurity system going forward. The remedial measures include agreeing to conduct a cybersecurity risk assessment of its information systems and after completion of the risk assessment, submitting the results along with an action plan to address discovered risks to the Department. The risk assessment results must contain all plans for updating or creating additional written polices and procedures to include (i) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing EyeMed; (ii) criteria for the assessment of the confidentiality, integrity, security and availability of EyeMed's information systems and NPI and (iii) criteria for the periodic assessments of any third-party service providers used by EyeMed.

Businesses subject to the New York Cybersecurity Regulation should carefully review their cybersecurity program and the requirements in the law to determine if they are in compliance with the cybersecurity requirements. If you have any questions regarding the New York Cybersecurity Regulation or need assistance in complying with the cybersecurity requirements, please let us know. ❑

✧ *Elizabeth Anstaett and Nathan Copeland*

LOOKING FOR A MARKETING AND PRIVACY COMPLIANCE RESOURCE? We publish an easy-to-use reference, our MARKETING AND PRIVACY DIGEST, that compiles the state laws governing financial privacy, fair credit reporting, telemarketing/automatic dialing and announcing devices, telephone monitoring and recording, electronic signatures and restrictions on the use of social security numbers by financial service providers. Creditors, marketers and servicers should find this resource invaluable to marketing and privacy program development and regulatory compliance. ***Contact us for details.***

FEDERAL RESERVE FINALIZES CARD-NOT-PRESENT RULE

The Federal Reserve Board recently finalized a rule in Regulation II preventing exclusive debit card networks in e-commerce transactions. The final rule requires a debit card issuer to configure each of its debit cards so that card-not-present transactions can be processed on at least two unaffiliated networks. A card-not-present transaction is a transaction where a debit card is not presented at a terminal to make a payment, such as payments

Darrell L. Dreher
ddreher@dltlaw.com

Elizabeth L. Anstaett
eanstaett@dltlaw.com

Nathan D. Copeland
ncopeland@dltlaw.com

Susan L. Ostrander
sostrander@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

Benjamin J. Hurford
bhurford@dltlaw.com

Mercedes C. Ramsey
mramsey@dltlaw.com

Judith M. Scheiderer
jscheiderer@dltlaw.com

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

made online, over the phone or through the mail.

While the final rule requires an issuer to enable at least two unaffiliated networks to process a debit card transaction, the final rule does not require an issuer to ensure that two unaffiliated network will actually be available to the merchant for every transaction. The final rule aims to ensure that merchants have the opportunity to choose from at least two unaffiliated networks when routing debit card transactions.

An example of prohibited network restrictions on an issuer's ability to contract with other payment card networks under the final rule includes: network rules or contract provisions limiting or otherwise restricting the other payment card networks that an issuer may enable on a particular debit card, or network rules or contract provisions that specify the other networks that an issuer may enable on a particular debit card.

An issuer should determine whether merchants have the opportunity in card-not-present debit card transactions to choose from at least two unaffiliated networks when routing debit card transactions to ensure compliance with the final rule. The final rule is effective July 1, 2023.

If you have any questions regarding the final rule or need assistance in complying with the final rule, please let us know. ❑

✧ *Elizabeth Anstaett and Nathan Copeland*