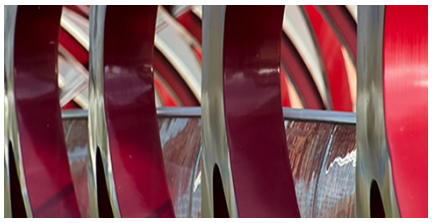
masuda funai



News & Types: クライアント・アドバイザリー

ビジネスメール詐欺（Business E-mail Compromise）への注意喚起

1/5/2022

By: ケントン クノップ

Practices: 商事／競争／取引, 訴訟

概要

サイバー犯罪の手段として、ビジネスメール詐欺（Business E-mail Compromise）の手法が好んで利用されるようになりました。悪意ある第三者は、支払の受領者になりすまして支払者を欺き、自らが管理する口座に資金が振り込まれるように企てます。このようなビジネスメール詐欺に関する事件に対して、裁判所は、詐欺による損害を回避することが最も期待できる立場にあり、かつ、損害の回避について合理的な注意を怠った当事者がその損害に対する責任を負うとする統一商事法典(UCC)の原則に注目するようになってきました。今日のビジネス環境で売買取引に携わる企業がビジネスメール詐欺の被害に遭わないようにするためには、顧客に対して、取引に関わる支払情報に変更があった場合は、実際に支払をする前の電話確認を欠かさないよう求めることが、これまで以上に重要となります。

メディアにおいては、サイバー犯罪が、熟練したハッカーが狙いをつけたコンピュータ・システムに巧みに侵入し、機密データや銀行口座の資金を盗み出すことであるかのように描写されます。しかし、実際のサイバー犯罪者は、ビジネスメール詐欺と呼ばれるごく単純な手口を使って、機密データや資金を盗み出すようになってきています。連邦捜査局(FBI)のインターネット犯罪苦情センター(Federal Bureau of Investigation Internet Crime Complaint Center)は、2020年インターネット犯罪報告書で、ビジネスメール詐欺に関して、同センターに送られた苦情件数は2020年だけでも19,369件に上り、その被害によって企業に引き起こされた調整後損失は18億ドルにも及ぶと述べています。また、それとは対照的に、2020年のランサムウェアによる損失は2,900万ドルにすぎないと述べています。

ビジネスメール詐欺の当事者は、通常、主にEメールを利用して事業を行っている二者と、その二者間に割り込み、かかる会社の従業員にフィッシングメールを送ったり、または他の不正手段を講じたりして、一方当事者のEメールアカウントに不正アクセスし、両当事者間のEメールのやりとりをひそかに監視する悪意ある第三者です。悪意ある第三者は、両当事者間のEメールのやりとりを監視し、それにより電信送金やACH(Automated Clearing House)送金により請求書の支払いや決済を行う時期が明らかとなった場合、支払受領者の実際のEメールアドレスに類似させた偽物のドメインから、同受領者のEメールアカウントを持つ担当

者を装って、支払者とのEメール通信に割り込みます。悪意ある第三者は、その支払振込先の銀行情報が変わったことを支払者に通知し、当該第三者が管理する別の銀行口座に支払を振り込むように指示します。そして通常の場合、支払者は、かかる新たな振込情報がそれまでずっと連絡し合っていた取引相手から送られたものであることを疑うことなく、その別の振込先に支払をすることになります。取引の当事者らが誤った銀行に支払金額が振り込まれたことに気づいたときには、当該悪意ある第三者は振り込まれた資金とともに消失しており、送金銀行や受領銀行でかかる資金を凍結したり、または取り戻したりするには手遅れとなっているのが一般的です。

ビジネスメール詐欺に遭った被害当事者が、未払いの債務をめぐって提起した訴訟において、裁判所は、誰が損失を負担すべきかを決定する際に、統一商事法典(UCC)（第3-404(d)条および第3-406条)に基づき、「債権の準占有者」（債権者らしい外観を有する者）と偽造有価証券について論じる伝統的なUCCの有価証券原則に着目しました。

2015年にビジネスメール詐欺に関してフロリダ州で提起されたある連邦訴訟事件は、原告／支払者が、被告／受領者からトラックを購入して、その代金を支払った際に、悪意ある第三者が管理する銀行口座に総額570,000ドルが流用されたというものでした。本件で裁判所は、UCC第3-404(d)条の「準占有者」規則を適用しました。本規則は、合理的な注意を払うことによって不正行為を防止することが最も期待できる立場にあり、かかる注意を怠った当事者が損害を負担すると定めています。裁判所は、受領者によるEメールアカウントの取り扱いに不注意があったために、第三者による不正行為が引き起こされたわけではないと判断し、実際には、両当事者のEメールアカウントがハッキングされており、どちらの当事者が最初にハッキングの被害に遭ったのか、どのようにハッキングされたのかは不明であると認定しました。そのうえで、裁判所は、原告／支払者が、通常とは異なる振込先を指示されたときに、合理的な注意を払い、実際に支払金額を振り込む前に、被告／受領者に電話をして確認すべきであったと述べました。そして、原告は、悪意ある第三者に支払いを行う前に、まず被告に電話確認をすることを怠ったため、詐欺に関連する損害は原告が負担するものと裁判所は判示しました。

同様に、2018年に連邦第6巡回区控訴裁判所で提起された訴訟事件も悪意ある第三者による支払の流用に関するものでしたが、同裁判所は、トライアル(trial)において、どの当事者が不正を防止することが最も期待できる立場にあったかを判断する必要があると判示し、トライアルでは、比較過失の原則(comparative fault principles)に基づいて損失を配分しました。

近時、ネバダ州やウエストバージニア州など他の裁判管轄で判決が下された事例でも、同様のビジネスメール詐欺に関する状況において「準占有者」の規則が適用されました。支払者は、受領者に電話し、通常とは異なった支払手続きについて確認し、損失を回避することが最も期待できる立場に置かれていたことから、損失に対する責任を負うべきであると裁判所は判示しました。

近時の判例法に照らしながらビジネスメール詐欺に関して考察してみると、裁判所は、企業のITセキュリティ対策が十分に実施されていたとしても、ビジネスメール詐欺のリスクを完全に排除することができないことを認識しており、最初に被害に遭った当事者が誰であったのかはあまり重視せず、代わりに、その被害による損

失を回避することが最も期待できる立場にあったとみなされる当事者に責任を課していることが明らかです。ほとんどの場合、損失を回避することが最も期待できる当事者とは、悪意ある第三者から通常と異なる支払指示を受け取った支払者であり、支払者は、支払金額を指示された口座に振り込む前に、受領者に電話し、その情報を確認することにより問題を解決することができます。

したがって、各企業は、業務手順を導入することが求められ、顧客に対して、顧客自身を保護するためにも、支払関連情報が変更された場合は、実際に支払をする前に、信頼できる電話番号に電話をして情報の変更を確認するよう注意を促すことが大切です。今日のハイテク環境において、ローテクな電話確認が、避けがたいビジネス・リスクに対する最も効果的な防衛策といえます。

本稿のビジネスメール詐欺についてご質問がある方、またはかかる詐欺に対する対応策についてさらに情報をご希望の方は、当事務所の弁護士までご連絡ください。