T.C. İSTANBUL
11 ASLİYE TİCARET MAHKEMESİ HÂKİMLİĞİNE

BİLİRKİŞİ HEYETİ RAPORU

DOSYA NO : **2020 / 275 Esas**
DAVACI : **SİMSİYAH TEKSTİL TURİZM SAN. TİC. LTD. ŞTİ**
VEKİLİ : **Av. Zeynep BALCI**
DAVALI : **YAPI VE KREDİ BANKASI A.Ş.**
VEKİLİ :**Av.Mert AYTEKİN&Av.Naz ATAKAY&Av.Zeynep GÜNALMIŞ**
DAVA KONUSU : **Tazminat (Haksız Fiilden Kaynaklanan)**

BİLİRKİŞİ KURULUNA TEVDİ EDİLEN GÖREV

Sayın Mahkemenin 20.01.2022 Tarihli ara kararında; davacı taraf iddiası, davalı taraf savunması, dosya kapsamındaki tüm bilgi ve belgeler incelenmek suretiyle bilirkişi incelemesinin yaptırılmasına karar verilmiştir.

I. TARAFLARIN İDDİA VE SAVUNMALARI

1.1 DAVACI TARAFIN İDDİALARI

Davacı Vekili dilekçesinde özetle;
Davacı SİMSİYAH TEKSTİL TURİZM SAN. TİC. LTD. ŞTİ'nin, Davalı Yapı ve Kredi Bankası'nın 4086430 numaralı müşterisi olduğu, DEMİRTAŞ OSB Şubesinde bulunan TR 91 0006 7010 0000 0080 9914 23 İban numaralı vadesiz hesabı aracılığı ile satış, tahsilat ve vergi ödemelerini gerçekleştirdiği,

Davacının davalı bankada bulunan bu hesabından 16.01.2019 tarihinde, Hüseyin Duman adına kayıtlı Yapı ve Kredi Bankası Arnavutköy Şubesi hesabına; saat 18:11:05'te 35.000 TL, saat 19:26:30'da 3.000 TL olmak üzere toplam 38.000 TL havale yapıldığı, yapılan havale işlemlerinin açıklamasına "kumaş boya ödemesi ve eksik ödeme devamı" yazıldığı (EK-1 Dekontlar ve banka hesap dökümü),
Davacı şirketin 30.01.2019 tarihinde dava konusu hesabından çekilen toplam 38.000 TL'nin iadesini talep etmek amacıyla davalı Bankanın Genel Müdürlüğü'ne, Teftiş Kurulu Başkanlığına ve DEMİRTAŞ OSB Şubesine ve Bankacılık Düzenleme ve Denetleme Kurulu Başkanlığı'na (BDDK), Bursa 25. Noterliğinden ayrı ayrı ihtarnameler gönderdiği (EK-2: Gönderilen ihtarnameler ve teblig şerhIeri), Sözkonusu ihtarnamelere ilişkin davalı bankanın; *"Itiraza konu işlemlerin tarafınıza ait kullanıcı kodu,* statik şi*fre ve sistemimizde kayıtlı telefonunuza gönderilen tek kullanımlık şifrenin internet bankacılığı sistemimize girilerek gerçekleştirildiği tespit edilmiştir. Bu durum cep telefonunuzun bağlı olduğu GSM şirketi tarafından da teyit edilebilir. Şifrenin saklanması/güvenli ortamlarda bankacılık işlemi yapılması ve cihaz güvenliğinin sağlanması sorumluluğunun yerine getirilmemesi nedeniyle, Bankamızın herhangi bir kusuru bulunmamaktadır. Çekilen tutar ile ilgili Bankamıza ödeme yapılamayacağı hususunu bilgilerinize sunarız."* şeklinde cevap vererek davacıya herhangi bir ödeme yapılamayacağının belirtildiği (EK-3: İhtarname cevapları) anlaşılmaktadır.

Davacı şirketin yıllardır bankacılık hizmetlerinden faydalandığı, gerekli güvenlik önlemlerinin bilincinde olduğu, dava konusu olayın gerçekleştiği tarihte, öncesi veya sonrasında şifre, parola gibi kişisel bilgilerini, üçüncü kişi veya kişilerle paylaşmadığı bu nedenle dava konusu banka hesabından başka bir hesaba para aktarılması sonucunda meydana gelen zarardan sorumlu tutulamayacağı,

Davalı bankanın müşterilerinin haberi olmadan bilgisayar korsanlığı yoluyla başka bir hesaba para aktarılmasının önlenmesi konusunda ek güvenlik tedbirleri alma yükümlülüğü bulunduğu, bankaların kendilerine yatırılan paraları mudilere istendiğinde veya belli bir vadede ayrı veya misli olarak iade etmekle yükümlü oldukları, usulsüz işlemle çekilen paraların aslında doğrudan doğruya bankanın zararı niteliğinde olup mevduat sahibinin bankaya karşı alacağının aynen devam ettiği, usulsüz işlemlerin gerçekleşmesi ispatlandığı takdirde mevduat sahibinin kusurundan sözedilebileceği belirtilerek; davacının dolandırıcılık nedeniyle uğramış olduğu maddi ve manevi zararlara karşılık şimdilik 38.000,00 TL maddi tazminatın, olay tarihi olan 16.01.2019 tarihinden itibaren işleyecek ticari faiziyle birlikte davalıdan alınarak davacıya ödenmesi talep edilmiştir.

<u>Davacı Vekili cevap dilekçesinde özetle;</u>
Davacının manevi tazminat yönündeki taleplerinin sehven yazıldığı kabul edilerek Sayın Mahkeme tarafından dikkate alınmaması gerektiği,

Davacıya gönderilen doğrulama kodu her ne kadar davacının cep numarasına gönderilmişse de, yapılan yönlendirme nedeni ile şifrenin davacıya değil yetkisiz 3.kişilere gittiği, ancak bu durumun Banka'nın şüpheli davranış ve hareketlerini tespit eden yazılım ve programlar aracılığıyla davacının bankacılık işlemleri için giriş yaptığı iz kayıtlarından farklı olarak bambaşka bir iz kaydının sisteme girişinin gerçekleştiğini tespit etme noktasında kusurunun oldukça açık olduğunu gösterdiği belirtilmiştir.

BDDK'nın 14.09.2007 tarihli "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ madde 3/1-ğ; Denetim izi: Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtları, ifade etmektedir. Madde 9/3; Bilgi sistemlerine erişim için kullanılan kimlik doğrulama verilerinin tutulduğu veritabanlarının güvenliğini sağlamaya yönelik gerekli önlemler alınır. Bu amaçla alınacak önlemler ……, **<u>yapılacak her türlü kontrolsüz değişikliği algılayacak sistemlerin kurulması</u>, yeterli denetim izlerinin tutulması ve bu denetim izlerinin güvenliğinin sağlanması** hususlarını içerir.
Madde 12/4; Bilgi sistemleri dâhilinde gerçekleşen kritik faaliyetlere ilişkin yetkilendirme veritabanları da dâhil olmak üzere **her türlü veritabanı, uygulama ve sistemde meydana gelecek değişiklik**, ekleme ve silmenin, kimlik doğrulaması uygun tekniklerle gerçekleştirilmiş **yetkili kullanıcılar tarafından yapılması sağlanır.** Bu kapsamdaki her türlü işlem için banka bünyesinde etkin bir değişiklik yönetimi tesis edilir, **yeterli denetim izi tutulur ve tutulan denetim izlerinin düzenli olarak gözden geçirilmesi sağlanır** Şeklindedir**..**

Mobil/İnternet/Telefon bankacılığı kullanımında kullanıcıların şüpheli davranış ve hareketlerini tespit edebilecek (Fraud Detection) yazılımlar ve programlar kullanılabilmektedir. Herhangi bir bankanın mobil/internet/telefon şube kanallarını kullanarak işlem yapan müşterisinin inkara imkan vermeyecek şekilde kendisini tanımlayacak yöntemleri uygulaması zaruridir. Davalı tarafın güvenlik tedbirlerinin alınması konusunda yetersiz kaldığı, mobil/internet/telefon üzerinden banka sistemlerine erişim sağlayabilen müşterisini yetkilendirilmiş kişi/yetki sahibi kişi olarak tanımlayamadığı ve bu nedenle bir açık söz konusu olduğundan bankanın sorumlu ve kusurlu olduğu şeklinde ifade edilmiştir.

1.2 DAVALI TARAFIN SAVUNMALARI

Davalı Vekili tarafından sunulan dilekçede özetle;
Davalı vekilinin davaya ilişkin hem usule hem de esasa ilişkin itirazlarının bulunduğu,

Dava konusu havale işleminde iddia edilenin aksine davalı bankanın davacıya akıllı SMS şifresini davacının davalı banka nezdindeki kayıtlı telefon numarasına gönderdiği, gelen şifrenin internet bankacılığı sistemine doğru girilmesiyle birlikte havale işleminin tamamlandığı, davalı tarafın akıllı SMS göndererek davacı tarafı bilgilendirdiği böylece mevzuata ve sözleşmelere uygun şekilde hareket ettiği ve işlemin gerçekleştiği beyan edilmiştir.

Bankalar'dan bu yönde gönderilen uyarıcı metinlere rağmen; davacının kullanıcı kodu + statik şifre + tek kullanımlık şifresine ulaşılmış olmasının bu bilgilerin güvenli bir şekilde muhafaza edilmediğini gösterdiği, davalı bankanın üzerine düşen sorumlulukları yerine getirdiği ve olayda herhangi bir kusurunun bulunmadığı, davacı tarafın şifrelerin korunması ve kendisine gönderilen akıllı SMS'lerin kimse ile paylaşılmaması gerektiği konusunda ihmalkar davrandığı ve basiretli bir tacirin göstermesi gereken dikkat ve özen sorumluluğunu yerine getirmediği, bu nedenle dava konusu uyuşmazlığa davacı tarafın kusurlu hareketlerinin yol açtığı belirtilmiştir.

Davalı bankanın uluslararası kabul gören ve uygulanan 3D Secure, sisteme girerken SMS gönderimi, Yapı ve Kredi Bankası internet şubesi dijital sertifikası, güvenlik kodu, sanal klavye, saldırı tespit sistemi, statik – dinamik şifre (mobil onay kodu), para çekimi ve hesap hareketlerini SMS veya sözlü veya mail ile olarak bildirmek (işlem onay kodu ile birlikte bu bilgi verilmektedir), elektronik imza, 128 bit SSL, firewall, anti phising ve sair programlar, teknikler ile gerekli önlemleri aldığı böylece davalı bankanın müşterilerine ilişkin güvenlik konularına dikkat ettiği, mevcut güvenlik önlemlerinin yanı sıra müşterilerine ekstra güvenlik ayarları tanımlama imkanı sağladığı; kullanıcıların internet bankacılığı üzerinden yapmak istediği işlemleri kısıtlayabildiği, internet bankacılığı üzerinden kullanmak istedikleri hesapları belirleyerek işlemlerini tercih ettikleri limitler dahilinde gerçekleştirebildikleri ve internet bankacılığı erişim ayarları ile sadece kendi belirledikleri zaman ve IP adreslerinden işlemleri gerçekleştirebildikleri, ayrıca güvenlik konuları ile ilgili müşterilerine düzenli olarak, bildirim, uyarı ve tavsiyelerde bulunulduğu belirtilerek yukarıda açıklanan sebeplerden dolayı davanını reddi talep edilmiştir.

II. DAVA DOSYASININ İNCELENMESİ

Davacı şirket, 16.01.2019 tarihinde, davalı bankadaki hesabından iki ayrı işlemde toplam 38.000 TL'nin dava dışı Hüseyin Duman isimli kişinin hesabına havale yapılmasının kendisinin izni ve onayıyla olmadığını, bu işlemden zarara uğradığını, davacının hesabındaki paranın güvenliğinin sağlayamaması nedeniyle uğranılan zarardan davalı bankanın sorumlu olduğu iddiasıyla işbu dava açılmıştır.

Davacının Yapı ve Kredi Bankası Demirtaş OSB Şubesi, 80991423 Numaralı Hesabının 16.01.2019-21.01.2019 Tarihleri Arası Hesap Ekstresi ve Banka Dekontları incelendiğinde;

Davacının, davalı banka nezdinde bulunan 80991423 Hesap Numaralı, TR91 0006 7010 0000 0080 9914 23 İban numaralı mevduat hesabından 16.01.2019 tarihinde, Hüseyin Duman adına kayıtlı Yapı

ve Kredi Bankası Arnavutköy Şubesi 55948047 Hesap Numaralı, TR54 0006 7010 0000 0055 9480 47 İban numaralı mevduat hesabına; saat 18:11:08'de 35.000 TL, saat 19:26:31'de 3.000 TL olmak üzere toplam 38.000 TL havale yapıldığı, yapılan havale işlemlerinin açıklamasına "kumaş boya ödemesi ve eksik ödeme devamı" yazıldığı ve dekontların da dava dosyasında bulunduğu görülmüştür. Davacı şirketin 30.01.2019 tarihinde dava konusu hesabından çekilen 38.000 TL'nin iadesini talep etmek amacıyla davalı Bankanın Genel Müdürlüğü'ne, Teftiş Kurulu Başkanlığına ve DEMİRTAŞ OSB Şubesine ve BDDK'ya Bursa 25. Noterliği'nden ayrı ayrı ihtarnameler gönderdiği; Davacı tarafın Bursa 25. Noterliği 29.01.2019 Tarih, 00892 yevmiye numaralı ihtarnamesi, Davalı Yapı ve Kredi Bankası A.Ş. İç Denetim Yönetimi Birimi tarafından hazırlanan Beşiktaş 19. Noterliği 08.02.2019 Tarih, 04187 yevmiye numaralı İhtarnamesi, BDDK Finansal Tüketici İlişkileri Daire Başkanlığı 15.02.2019 Tarihli, 47916912-622.01[01-50]-E2253 Sayılı İhtarnamesinin, (EK-2: Gönderilen ihtarnameler ve tebliğ şerhleri) dava dosyasında yer aldığı anlaşılmaktadır.

Davalı banka ve ilgili birimlerine gönderilen ihtarnamelerde; davacı taraf "…*Bankanız tarafından söz konusu havale işlemleri gerçekleştirilirken; banka hesabıma tanımlı 0554 587 18 38 numaralı şirket hattına onay kodu/şifresi gönderilmemiş ve tarafımca herhangi bir şekilde onay verilmemiştir.*
Banka hesabımdan bilgim ve rızam dışında 2 seferde havale edilen toplam 38.000,00 TL'nin 16.01.2019 tarihinden itibaren işleyecek ticari faizi ile birlikte….iade edilmesi" talep etmiştir.
Sözkonusu ihtarnamelere ilişkin davalı banka ve ilgili organları; *"Itiraza konu işlemlerin tarafınıza ait kullanıcı kodu,* statik şi*fre ve sistemimizde kayıtlı telefonunuza gönderilen tek kullanımlık şifrenin internet bankacılığı sistemimize girilerek gerçekleştirildiği tespit edilmiştir. Bu durum cep telefonunuzun bağlı olduğu GSM şirketi tarafından da teyit edilebilir. Şifrenin saklanması/güvenli ortamlarda bankacılık işlemi yapılması ve cihaz güvenliğinin sağlanması sorumluluğunun yerine getirilmemesi nedeniyle, Bankamızın herhangi bir kusuru bulunmamaktadır. Çekilen tutar ile ilgili Bankamıza ödeme yapılamayacağı hususunu bilgilerinize sunarız."* şeklinde cevap verdiği görülmüştür.

Davacı şirket dava konusu işlemden sonra davalı Bankaya hesaplarını kapama talebinde bulunduğunu, ancak davalı Bankanın "Tüzel Kişiliğe Sahip Müşterilerden Alınacak Vadesiz Hesap Kapama Talimatı ve Ibranamesi"nde yazılı 2 durumdan birinin işaretlenmesi suretiyle kapatılabileceğini içeren bir ibraname sunulduğu, nihai olarak davacının imzalamadığı görülmektedir (EK-4: Tüzel Kişiliğe Sahip Müşterilerden Alınacak Vadesiz Hesap Kapama Talimatı ve Ibranamesi).

09.06.2020 Tarihli Hukuk Uyuşmazlıklarında Dava Şartı Arabuluculuk Son Tutanağı incelendiğinde; Davacı ve davalı tarafın 05.03.2020 – 09.06.2020 tarihleri arasında biraraya geldiği ancak tarafların müzakereler sonucunda Ticari Uyuşmazlığından Kaynaklanan Maddi Tazminat konusunda anlaşmaya varamadıkları görülmüştür.

Davacı vekilinin Sayın Mahkemenin 6 Nolu Ara Kararına ilişkin 08.04.2021 tarihli beyan dilekçesinde özetle; Davacı şirketin, 16.01.2019 tarihinde Yapı Kredi Bankasi'nın 4086430 müşteri numaralı, DEMIRTAŞ OSB Şubesinde bulunan TR 91 0006 7010 0000 0080 9914 23 İban numaralı vadesiz hesabından, Hüseyin Duman adına kayıtlı Yapı Kredi Bankası Arnavutköy Şubesi hesabına;

- saat 18:11:05 de 81.213.163.201 Ip ve 56861 Port numarasıyla 35.000 TL,
- saat 19:26:30 da aynı Ip ve 59264 Port numarasıyla 3.000 TL'nin havale yapıldığı,

Davacı şirketin hesabına tanımlı 0541 288 14 43 numaralı hattın olay tarihinde şifre ile giriş yapılan WEB üzerinden 0537 845 23 04 numaralı hatta yönlendirildiği ve bu numaranın Libya Vatandaşı Walid Khayrı Ab Al Masrı adına kayıtlı olduğunun anlaşıldığı,

Davacı şirket hesabına bilişim sistemiyle ulaşım sağlanan 81.213.163.201 IP ve 56861-59264 Portların Ahmet Yılmaz adına kayıtlı Bayrampaşa İstanbul adresindeki mukim…ve …nolu telefon aboneliğine ait olduğu Türk Telekom tarafından bildirilmiştir.

16.01.2019 olay tarihi itibariyle 0541 288 14 43 numaralı hatta ait sisteme giriş yapan kullanıcı bilgileri, sisteme giriş saatleri, ekran girişlerine ilişkin bilgileri, IP ve Log kayıtlarına ilişkin bilgileri de dahil olmak üzere hertürlü denetim iz kayıtlarının ve olay tarihi itibariyle davalı bankanın kullanıcıların şüpheli davranış ve hareketlerini tespit edebilecek hangi sistemleri kurduğu ve hangi teknik ve idari tedbirleri aldığı davalı bankadan talep edilmiştir.

III. DEĞERLENDİRME

1- BDDK'nın Dinamik Şifre İle İlgili Kararı

Bankacılık Düzenleme ve Denetleme Kurumu'nun ' Bankalardaki Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliği 14.9.2007 tarih ve 26643 sayılı Resmi gazetede yayımlanarak 1.1.2008 tarihinde yürürlüğe girmiş olup, Tebliğ'in Geçici 1' inci Maddesiyle, bankalara uyum için azami 2 yıl süre verildiğinden, anılan Tebliğ 1.1.2010 tarihinde bütün hükümleriyle yürürlüğe girmiştir.

Bu çerçevede, Tebliğin Üçüncü Kısım / Birinci Bölüm / İnternet Bankacılığı / Madde 27 / Fıkra 4 ile;

' … müşterilere uygulanan kimlik doğrulama mekanizması bir birinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen: müşterinin ' bildiği', müşterinin ' Sahip Olduğu ' veya müşterinin ' Biyometrik bir karakteristiği olan ' unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Müşterinin ' bildiği ' unsur olarak ' parola / değişken parola bilgisi gibi bileşenler, ' sahip olduğu unsur ' olarak **tek kullanımlık parola üretim cihazı, kısa mesaj servisi** ile sağlanan tek kullanımlık parola gibi bileşenler **kullanılabilir.** Bileşenler tamamen müşterinin şahsına özgü olmalı ve bunlar sunulmadan kişilik doğrulama gerçekleştirilmemeli, hizmete erişim sağlanmamalıdır… '
şeklinde düzenleme getirilmiştir.

Böylece, daha önce, internet bankacılığında dinamik şifre kullanılmasını zorunlu tutmayan **bankalar** kamu otoritesinin zorlamasıyla, **internet bankacılığı işlemlerinde dinamik şifre kullanmaya mecbur tutulmuşlardır.**

2- Yıllar İtibarıyla İnternet Bankacılığı Dolandırıcılıklarının Seyri

Ülkemizde, internet bankacılığı kullanımının yaygınlaşmaya başlamasıyla birlikte, özellikle 2003 yılı sonlarından itibaren, internet bankacılığı işlemlerinde dolandırıcılıklar görülmeye başlanmış ve takip eden yıllarda hesap sahipleri ile bankalar arasında doğan ihtilaflardan kaynaklanan binlerce dava (Alacak ve Ceza Davaları) tarafları ve Mahkemeleri meşgul etmeye başlamıştır.

İnternet, birden fazla haberleşme ağının (network) birlikte meydana getirdikleri bir iletişim platformudur. Bilgisayar yardımıyla kullanıcının yarattığı veriler yine bu araçlar yardımıyla belirlenen yerlere internet yapısı kullanılarak ulaşır. İnternet bu çok taraflı ve sınırlar ötesi erişim karakteri, güvenlik sorunları başta olmak üzere hukuksal ve teknik sorunları da beraberinde getirmiştir.

İnternet bankacılığı dolandırıcılıkları :

1) Dolandırıcıların, müştekinin (hesap sahibinin) bilgisayarına erişerek, banka ve Hesap bilgilerini ele geçirmesi,
2) Ele geçirilen bilgilerle, bu defa, bankanın ana bilgisayarındaki müştekinin hesabına Erişilmesi,
3) Müştekinin hesabının izlenmesi, bakiye olduğunda hesabın boşaltılarak, paranın Çekilebilecek bir hesaba aktarılması,
4) Nihai aktarma hesabından paranın çekilmesi

Şeklinde olmak üzere genel olarak 4 aşamada gerçekleşmektedir.

Not : Ceza davalarında yargılananlar, genellikle 4. Aşamadaki -ayakçı diye tabir edilen- kişiler olmaktadır.
IP erişim bilgilerindeki zaafiyet – ileride bilgi verileceği üzere- nedeniyle, 2 ve 3 safha ile ilgili olarak sağlıklı bir tespit pek mümkün gözükmemektedir.
Müştekiye ait bilgisayar (hard disk) incelemelerinde de bir tespit yapılamamaktadır.

Her dolandırıcılık hadisesinden sonra, bankaların, zaman içerisinde değişen;

- Şifre
- Ek parola
- Güvenlik kodu
- Sanal klavye
- IP kısıtlama
- Zaman Kısıtlama
- Hesap Kısıtlama
- Miktar Kısıtlama

Şeklinde (listenin uzatılması mümkündür) ek tedbirler alarak, dolandırıcılarla mücadele etmeye çalıştıkları, ancak, temelde, işlemlerin statik şifre ile yapılmasına izin verilmesinden kaynaklanan zafiyet nedeniyle, dolandırıcılıklar uzun yıllar devam etmiştir.
Zira, mesafeli bir işlem niteliğindeki (yüz yüze olmayan: non face to face) internet bankacılığı ilişkisinde müşteri tanıma (kimlik belirleme) yöntemindeki zaafiyetin yanı sıra, kullanıcı (bankadaki hesap sahibi) tarafında da önlenmesi tam olarak olası olmayan zayıflık söz konusudur : kullanıcılara ait bilgisayarlar, çeşitli açılardan dışarıdan müdahaleye ve ele geçirilmeye açıktır . Bu çerçevede;

- Uluslararası literatürde **‘phishing’** adı verilen yöntemle, bilgisayar kullanıcısına, sanki kendi bankasından geliyormuş intibasını veren bir e-posta gönderilmekte ve bu e-postada, mesela bilgilerin güncelleneceğinden bahisle, kullanıcıya ait çeşitli bilgilerin yanı sıra, internet şifreleri de istenmektedir.
- Bu e-postada bulunan ve bilgisayar kullanıcısını bankasının web sayfasına aktardığını düşündüren bağlantı linki, aslında bankanın web sayfasının taklidi olan sahte bir sayfaya yönlendirmektedir.

Bilgisayar kullanıcısı bu e-postayı cevaplamakla, dolandırıcılığın başlamasına zemin hazırlamaktadır.

- Normal gözüken bir e-postanın ekinin (exe uzantısının) açılması yönteminde **(DNS – Spoofing)**, bilgisayar kullanıcısından doğrudan doğruya bilgi istenmesi söz konusu değildir. Ancak e-posta ve ekinin açılması (tıklanması) halinde, kullanıcının bilgisayarına bir virüs veya Truva atı (trojan horse) yerleştirilmekte ve bu yöntemle, kullanıcının yaptığı işlemler kopyalanıp, kullanıcının bilgisayarı tarafından otomatik olarak dolandırıcıların bilgisayarına gönderilmektedir.

- Bir başka yöntem olan **keylogger** yönteminde, kullanıcının bilgisayarının klavyesinde yaptığı bütün işlemler – sanal klavye ve bilgisayar ekran görüntüleri dahil – kopyalanmakta ve dolandırıcının e-mail adresine otomatik olarak gönderilmektedir.

Not : Örnekler tahdidi değildir, çok fazla sayıda yöntem bulunmaktadır.

Öte yandan, internet bankacılığı ilişkisindeki ‘ banka’ tarafında şifre ve bilgilerin güvenliği konusunda zayıflık bulunduğunun öne sürülmesi pek mümkün gözükmemektedir.

Zira, şifreleme ve güvenlik yazılımları bilgilerin gizliliğini sağlamak amacıyla geliştirilen güvenlik yöntemleridir. Elektronik bankacılık faaliyetlerinde internet bankacılığı şubesinin güvenliği , siteye giriş ve çıkış noktalarının denetlenmesine yarayan firewall (güvenlik duvarı) ve SSL (Secure Socket Layer) şifreleme protokolü teknikleri ile sağlanmaktadır.

Bu çerçevede, internet bankacılığı hizmeti veren davalı bankalarda da (keşfen yapılan incelemelerden) dahil olmak üzere, bankaların güvenlik sistemlerinin, sistem bilgisayarının ve dolayısıyla siteye giriş ve çıkış noktalarının firewall (güvenlik duvarı) yazılımları ile korunduğu ve müşterilere ait şifre gibi kişisel bilgilerin iletişim seviyesinde 128 Bit’lik SSL (Secure Socket layer) şifreleme teknikleri ile şifrelenmiş olarak iletildiği ve anabilgisayarda da şifrelenmiş olarak (3DES) muhafaza edildiği bilinmektedir. Dolayısıyla, banka sistemlerinin geliştirilmiş yazılımlarla da korunması sebebiyle **3. Kişilerin, banka sistemine sızarak** müşteriye ait kişisel **bilgileri ele geçirmesi ve çözmesi** ihtimal dışı bir durum olarak görülmektedir.

Benzer prensiplerle, **iletişim ortamının güvenliği de sağlanmaktadır**. İnternet tüm bireylere açık bir iletişim aracıdır. Şifreleme, internet üzerinden aktarılan bilgilerin gizliliğinin sağlanması amacı ile geliştirilen bir güvenlik yöntemidir. İnternet bankacılığı uygulamalarında müşteri ile banka sistemi arasındaki bilgi alış verişi şifrelenmiş olarak gerçekleşir. Müşteri kişisel bilgilerinin kullanıcı bilgisayarı ile banka sistemi arasında 3. Kişilerin eline geçmemesi için bankaların sisteminde, tüm dünyada kullanılan 128 bit’lik SSL şifreleme tekniği kullanılmaktadır. Şifrelenmiş bu tür verilerin çözümü çok zor ve zaman alıcı, üst düzey teknik bilgi birikimi ve son derece yüksek maliyetler gerektiğinden, dava konusu olaylarda, **şifrelenerek giden kişisel bilgilerin iletişim ortamında ele geçirilip çözülmüş olması ihtimal dahilinde görülmemektedir.**

3- Yargıtay 11. Hukuk Dairesinin İçtihatlarıyla Oluşan Hukuki Altyapı ve 21.1.2012 Tarihli Yargıtay Hukuk Genel Kurul Kararı

İnternet Bankacılığı ihtilafları ile ilgili davalarda, bazen bankaları, bazen hesap sahiplerini sorumlu tutan, zaman zaman da bankaları kusurlu, hesap sahiplerini ise çeşitli oranlarda

müterafik kusurlu bulan Mahkemeler tarafından verilmiş olan kararlardan sonra, **Yargıtay 11. Hukuk Dairesi tarafından :**

‘ internet bankacılığı sistemini kurup hizmete sunan **bankanın** mudiinin kastı, kötü niyeti ve suç sayılır eylemini kanıtlayamayacağı sürece kendisine **emanet edilen paradan güven kuruluşu olması nedeniyle sorumlu olacağı**, sorumluluğun olağan sebep sorumluluğu olup, gerekli özeni gösterse bile zararın gerçekleşeceğini ispat etmesi durumunda sorumluluktan kurtulabileceği … ‘ (7.2.2008, 2008/ 1205)

‘ … davalı taraf savunmasında, internet bankacılığı şifrelerinin davacı müşteriden ele geçirildiğini savunmuş ise de, kanıt yükü kendisinde bulunduğu halde bu savunmasını kanıtlayamamıştır … **bankanın davacının hesabından çekilen paranın tamamından sorumlu tutulması gerekir** … ‘ (28.9.2009, 2009/9715)

Davalı banka internet bankacılığında kendisinin ve müşterilerinin güvenliğini sağlayacak **güvenlik enstrümanlarının kullanılmasını zorunlu kılmayıp**, somut olayda **davacının insiyatifine bırakması zararın doğmasında başlıca etken olup, davalı bankanın zarardan sorumlu** olduğu açıktır.
Bunun yanında, davacıya güvenlik enstrümanlarını kullanmadan işlem yapma yetkisinin davalı banka tarafından verilmiş olması karşısında, bunları kullanmadan işlem yapan davacının meydana gelen zararda müterafik kusurlu olduğunun kabulü de mümkün değildir … ‘ (2008/5076 – 2010/1134)

Şeklindeki ve benzer çok sayıdaki Kararlarıyla, belli bir içtihadı oluştuğu görülmektedir.

Öte yandan, **T.C Yargıtay Hukuk Genel Kurulu** tarafından verilen 21.11.2012 tarihli Karar’la (E.2012/11-550 K.2012 / 280):

‘ … somut olayda davalı **banka**, davacının müterafik kusurunu ve suç teşkil edebilecek eyleminin varlığını da kanıtlayamadığından davacı **mudinin kendisine tevdi ettiği mevduatı aynen iade etmekle yükümlüdür… ‘**

Denilerek, **müterafik kusur kararında direnilmesi kararının usul ve yasaya aykırı olduğu**na dair Karar verilerek, Yargıtay 11. Hukuk dairesi tarafından bozulan ‘ müterafik kusur kararları ‘ paralelinde içtihat tespit ettiği görülmektedir.

4- Cep Telefonlarına Ait SİM Kartlarının Klonlanması Olaylarından Sonraki Durum ve Yargıtay Kararları

İnternet bankacılığı hadiselerinde, **bankaların, Cep telefonlarına, SMS ile** tek kullanımlık şifre (**dinamik şifre** - değişken şifre) **gönderme uygulamalarının**, **SİM kartların klonlanması suretiyle aşıldığı**, dava dışı çok sayıda tanzim etmiş olduğumuz Bilirkişi Raporlarımızdan bilinmektedir.

Bu yöntemde, mudinin cep telefonu **operatörü** (Turkcell/Vodafone/Türk Telekom) **bayisine ‘ yeni bir SİM kart almak istiyorum** ‘ diye müracaat edilmekte ve **sahte mudi kimliğiyle yeni bir SİM kart alınmakta** ve gerçek mudideki SİM kart otomatik olarak kullanılamaz hale gelmekte ve bloke olmaktadır.

Dolayısıyla, **bankanın mudisine gönderdiğini zannettiği** SMS yoluyla gönderilen **dinamik şifre dolandırıcının elindeki cep telefonuna gönderilmiş olmaktadır.**

Meydana gelen çok sayıdaki ihtilaf ve davalardan sonra **Yargıtay 11. Hukuk Dairesi** tarafından verilmiş olan **Kararında** (2010/2208 E. 2011/12509 K.) , olayın GSM şirketi ile ilgili yönü açısından :

‘ … GSM şirketinin abone merkezinden **SİM kartın** kaybedildiğinden bahisle s**ahte kimlikle yeniden çıkartıldığı**, şirketin kimlik kontrolü yapmadığı, SİM kartın yetkisiz kişilerin eline geçmesini engellemek için gerekli önlemleri almadığı gerekçesiyle kusurlu kabul edilmiştir. Oysa dava konusu olayda davacının banka hesabında bulunan para 3. Kişiler tarafından rızası hilafına alınmış olup, **dolandırıcılık eylemi bankaya karşı işlenmiştir**… banka müşterisi olan davacının açmış olduğu **böyle bir davada GSM şirketi aleyhine hüküm kurulması doğru değildir** … **yanılgılı değerlendirmelerle aleyhine hüküm kurulması doğru bulunmamış …’**

denilerek, **Banka ve GSM şirketinin müştereken ve müteselsilen sorumlu olduğuna dair** verilen **kararın bozulduğu** anlaşılmaktadır.

Not : Benzer çok sayıda İçtihat bulunmaktadır.

Öte yandan, SİM kart klonlanması olaylarına karşı, **bankaların tedbir alarak SİM kart değişikliği yapılması halinde** internet bankacılığı **hizmetini bloke etmeleri** ve hesap sahibinin ATM e giderek blokeyi bizzat çözme zorunda bırakılmalarından **sonra, bu defa dolandırıcıların başka yöntemler buldukları** (somut hadiselerden ve basına akseden olaylardan) anlaşılmaktadır.

Bu çerçevede, zaman içerisinde ; **Bankaların, SİM kart değişikliklerinde tedbir almaya başlamalarından sonra** (2013 yılı başları), dolandırıcıların**, bu defa**, kart sahiplerinin elindeki **cep telefonunu hedefleyerek , çeşitli hile ve kandırmalarla** (x), banka tarafından gönderilmiş olan **tek kullanımlık şifreleri ele geçirmeye başladıkları** – tanzim ettiğimiz Bilirkişi Raporlarımızdan ve medyaya akseden olaylardan - bilinmektedir.

(x) : Hile ve kandırmalar çok çeşitlidir ve literatürde bu durum
‘ Oltalama ‘ (phishing) olarak adlandırılmaktadır;

. geriye doğru 10 yıllık kart ücretini iade edeceğiz,
. sigorta pirimi iade edeceğiz,
. hesabınız saldırıya uğramış, işlemleri iade edeceğiz,
. kartınız kopyalanmış, işlemleri iade edeceğiz,

bunun için, **cep telefonunuza gelecek olan mesajı lütfen bizimle paylaşınız…**

Not : Geçmişte yapmış olduğumuz Bilirkişi Raporlarından alıntı olup, tahdidi değildir, örnekleme yapılmıştır.

Yeni yöntemde, dolandırıcılar, mağdurun güvenini sağlamak üzere, mağdurun cep telefonunda arayan numara (x) olarak bir bankaya ait çağrı merkezinin (veya 155 Polis hattının) telefon numarasının **çıkmasını sağlamaktadırlar.**

(x) : İnternet ortamında, bu işleme imkan veren ve bedava temin edilmesi mümkün çok sayıda uygulama olduğu görülmektedir.

5- Yargıtay 19.Hukuk Dairesinin 19.4.2016 Tarihli İlamı

Anılan BOZMA İlamında ;

‘ … davacı, banka kredi kartı hesabından usulsüz çekilen paranın tazmini istemiyle bu davayı açmıştır. Dosyadaki bilgilerden ve özellikle davacının savcılıktaki ifadesinden, davacının telefonla aranması sonucunda kart bilgilerini verdiği ve bunun sonucunda cep telefonuna gelen şifrelerini de karşı taraf bildirdiği anlaşılmaktadır. Bankalar, bir güven kurumu olduğundan, mudilerinin kendilerine emanet ettikleri parayı korumakla yükümlüdürler. Bu durumlarda, hafif kusurlarından dahi sorumludurlar. Ancak, somut olayda **davacının kart bilgilerini ve şifreleri karşı tarafa kendisi bildirdiğinden ve bu bilgilere göre işlem yapıldığı anlaşıldığından, bankanın zarardan sorumlu olduğu kabul edilemez.** Mahkemece bu hususlar gözetilerek davanın reddine karar verilmesi gerekirken, yazılı şekilde hüküm kurulması doğru olmamış, mahkeme kararının bozulması gerekmiştir…’

denilerek Mahkemece verilmiş olan Kararın bozulduğu anlaşılmaktadır.

6- Dava Konusu Hadise

a) Taraflar Arasındaki İlişki ve İhtilaflı işlemler

- Davacı SİMSİYAH TEKSTİL TURİZM SANAYİ TİCARET LDT.ŞTİ. yetkilisi Tarık Balcı’nın davalı YAPI ve KREDİ Bankası A.Ş.’ nin müşterisi olduğu ve davalı bankanın 910-Demirtaş OSB Şubesi nezdinde 80991423 numaralı vadesiz TL hesabının bulunduğu,

- Davacı’nın davalı Yapı ve Kredi Bankası A.Ş Demirtaş-OSB şubesi nezdindeki 80991423 numaralı vadesiz hesabından 16.01.2019 tarihinde:

Saat	**Tutar**	**Açıklama**	**IP Adresi**
18.11.05	35.000 TL	SendHavale	**81.213.163.201**
19.26.30	3.000 TL	SendHavale	**81.213.163.201**

Şeklinde olma üzere davacının hesabından 2 işlemde toplam 38.000.- TL nin davalı banka nezdinde bulunan 55948047 numaralı hesaba havale yolu ile gönderilmiş olduğu,

- Anılan ihtilaflı işlemlerin internet bankacılığı üzerinden gerçekleştirilmiş olduğu,

- Anılan işlemlerin internet bankacılığı üzerinden gerçekleşebilmesi için gerekli ve şart olan tek kullanımlık (dinamik / her işlemde değişen) SMS şifrelerinin aynı gün 16.01.2019 tarihinde:

Saat	**Mesaj Gövdesi**
18.08	Akıllı SMS sifrenizi banka personeli dahil kimseyle paylasmayiniz/tuslamayiniz. Kurumsal Internet/Mobil subeye giris icin tek kullanimlik sifreniz: ****
18.10	Akıllı SMS sifrenizi banka personeli dahil kimseyle paylasmayiniz. İsleminizi gerceklestirmeniz icin sifreniz: ****
19.26	Akıllı SMS sifrenizi banka personeli dahil kimseyle paylasmayiniz. İsleminizi gerceklestirmeniz icin sifreniz: ****

Şeklinde olmak üzere gerek internet bankacılığın a girişte ve gerekse para çıkışında davalı banka tarafından davacıya ait olan 0541 288 14 43 numaralı cep telefonuna başarılı bir şekilde gönderilmiş olduğu,

b) İhtilaflı İşlemlerin Yapılmış Olduğu IP Adresi

- Davacı'nın davalı Yapı ve Kredi Bankası A.Ş nezdindeki hesaplarına internet üzerinden erişimde kullanılmış olan IP adresinin işlem tarihi ve saatinde dinamik veya statik IP havuzundan hangi telefon abonesine tahsisli olduğunun ancak bir Savcılık soruşturması ile tespit edilebileceği,

- Zira mevzuat gereği olarak servis sağlayıcıların Hukuk ve İdare mahkemelerinin taleplerini içerik yönünden yanıtlamadıkları,

- T.C Bursa Cumhuriyet Başsavcılığı'nın 2019/51966 CBS dosyasında;

    - İşlemlerde kullanılan **81.231.163.201** numaralı IP adresi ve 56861-59264 portların Ahmet Yılmaz adına kayıtlı Bayrampaşa İstanbul adresinde mukim Kartaltepe Mah. Mercan Cad. No:24 adresindeki 0212 614 3059 nolu telefon aboneliğine ait olduğunun Türk Telekom tarafından bildirildiği,

- Müşteki hesabına tanımlı 0541 *** 1443 numaralı hattın ise; olay tarihinde şifre ile giriş yapılan WEB üzerinden **0537 845 23 04 numaralı hatta yönlendirildiğinin belirlendiği**, 0537 845 23 04 numaralı telefonun Libya vatandaşı Walid Khayrı Ab Al MASRI adına kayıtlı olduğu,

Bilgilerinin iddianame içerisinde yer aldığı tespit edilmiştir.

IV. SONUÇ

Raporumuzun önceki bölümlerinde verilen bilgiler ve yapılmış olan tespitlere göre:

- Davacı'nın davalı Yapı ve Kredi Bankası A.Ş 910-Demirtaş OSB Şubesi nezdinde 80991423 numaralı hesabından 16.01.2019 tarihinde toplam 38.000,00-TL nin davalı banka nezdindeki Hüseyin Duman adına kayıtlı hesaba havale yolu ile olmak üzere aktarılarak çekilmiş olduğu,

- Anılan ihtilaflı işlemlerin internet bankacılığı üzerinden gerçekleştirilmiş olduğu,

- Anılan işlemlerin internet bankacılığı üzerinden gerçekleşebilmesi için gerekli ve şart olan tek kullanımlık (dinamik / her işlemde değişen) internet bankacılığına giriş şifresinin aynı gün 16.01.2019 tarihinde davalı banka tarafından davacıya ait olan 0541 288 14 43 numaralı cep telefonuna başarılı bir şekilde gönderilmiş olduğu,

- Bursa Cumhuriyet CBS tarafından davacıya ait telefon numarasının olay tarihinde Libya Vatandaşı Walid Khayrı Ab Al MASRI adına kayıtlı 0537 845 23 04 numaralı telefon hattına yönlendirilmiş olduğunun belirlendiği,

- Dolayısıyla her işlemdeki tek kullanımlık şifrelerin davacıya değil de yönlendirme yapılmış olan 537 845 23 04 numaralı cep telefonu hattına gitmiş olduğu,

- Ülkemizde yıllarca devam eden SIM kopyalama olaylarında bankalarca tedbir alınarak (sahte kimlikle) SIM kart değişikliği yapıldığında, internet bankacılığı hizmetinin durdurularak hesap sahibinin bir ATM de kartı ve şifresi ile yüz yüze yapılacak bir işlemle SIM blokesini çözme tedbiri alınmış olduğu,

- Son yıllarda huzurdaki uyuşmazlıkta olduğu gibi cep telefonunun başka bir cep telefonu numarasına yönlendirilmesinden kaynaklanan uyuşmazlıklarının artmaya başladığı,

- SIM kart değişikliği hallerinde bankalar ile cep telefonu operatörleri arasında sağlanan bilgi akışının, cep telefonunun başka bir numaraya yönlendirilmesinde de yapılmamasının ***davacı bankanın ağır bir kusuru olduğu***, *yönlendirme yapıldığında internet bankacılığı hizmetinin bloke tutularak blokenin sağlıklı bir şekilde çözülmesinin sağlanmasının davacı bankanın sorumluluğunda olduğu*,

- ***Davacının*** *gerek GSM operatöründen gelen şifreyi gerekse davalı bankadan gelen internet bankacılığı giriş şifresini oltalamaya yakalanarak dolandırıcılara kaptırmakla* ***kusurlu olduğu***,

- ***Davacının kusurunun davalı bankanın cep telefonu numarasının başka bir cep telefonu numarasına yönlendirilmesi hallerindeki ağır kusuru nedeniyle arka planda kaldığı, bu nedenle davacıya müterafik kusur yöneltilme imkanı gözükmediği***,

- Yerleşik Yargıtay içtihatlarında, hesap sahibi ile banka arasında çıkan internet bankacılığı dolandırıcılıkları uyuşmazlıklarında sahte kimlikle yapılan SIM kart yenilemelerinde cep telefonu operatörlerine yöneltilen müterafik kusur kararlarının dahi uygun görülmediği,

- Bankaların kendi takdirlerinde olmakla birlikte tek kullanımlık **şifreyi cep telefonuna gönderme uygulamalarının:**

- Başkasına ait (Türkcell, Vodafone, Türk Telekom.vs.) bir alt yapının kullanılması,
- Bu alt yapının, çeşitli hile ve kandırmalara açık olduğu gibi, telefona virüs bulaştırma ve huzurdaki davada olduğu gibi başka bir telefon numarasına yönlendirme,

gibi nedenlerle elektronik imza kanununda tariflenen e-imza, Mobil İmza veya şifre üreten şifrematik cihazları kadar güvenli bir yöntem olmadığı,

- Davalıya ait statik internet bankacılığı bilgilerinin nasıl ele geçirildiği noktasında bir tespit yapılabilmesi imkanı gözükmediği,

*hususlarından hareketle ve **takdiri tamamen Mahkemeye ait olmak** ve hiçbir bağlayıcılığı olmamak üzere**, davacı** tarafından 38.000.00- TL üzerinden yapılmış olan **alacak talebinin yerinde olduğu** tespit ve kanaatine ulaşılmaktadır.*

Keyfiyeti, 6100 sayılı HMK 282 hükmü de gözetilmek kaydıyla ve HUMK 266/c.2 uyarınca bilcümle hukuki tavsif ve takdir tamamıyla ve münhasıran sayın yargı makamına ait olarak, yüce Mahkemenin değerlendirmesine saygıyla arz ederiz. 18.07.2022

BİLİRKİŞİ KURULU

Prof.Dr. Gülcan ÇAĞIL
Marmara Üniversitesi
Öğretim Üyesi

Altuğ GÜRGÜL
Bilgisayar Mühendisi