Sectorul Serviciilor Financiare
Buletin informativ

Autoritatea Bancară Europeană („ABE") a emis un Ghid final privind securitatea plăților pe internet („Ghidul")

La data de 19 decembrie 2014, ABE a publicat Ghidul final privind securitatea plăților pe internet menit să stabilească un set de cerințe minime în domeniul securității serviciilor de plată oferite prin intermediul internetului (servicii de plată pe internet). Ghidul a fost emis ca răspuns la nivelul ridicat de fraudă incident la nivelul serviciilor de plată pe internet, având data limită de implementare 1 August 2015. Cerințe mai stricte urmează să fie implementate la un moment ulterior, în baza viitoarei Directive privind serviciile de plată 2.

Ghidul se bazează pe dispozițiile Directivei 2007/64/CE cu privire la serviciile de plată („Directiva privind serviciile de plată") referitoare la cerințele de informare pentru serviciile de plată și obligațiile prestatorilor de servicii de plată. Trebuie menționat că pe lângă cerințele minime prevăzute în Ghid, este responsabilitatea prestatorilor de servicii de plată să monitorizeze și să evalueze riscurile implicate de operațiunile lor de plată, să își dezvolte propriile politici detaliate de securitate și să pună în aplicare măsuri proporționale cu riscurile inerente serviciilor de plată prestate. Autoritatea competentă poate decide să solicite prestatorilor de servicii de plată să raporteze autorității competente dacă îndeplinesc condițiile prevăzute de Ghid.

Domeniu de aplicare. Ghidul se adresează instituțiilor financiare, astfel cum sunt definite la art. 4 alin. (1) din Regulamentul nr. 1093/2010, și autorităților competente, astfel cum sunt definite la art. 4 alin. (2) din Regulamentul nr. 1093/2010 și sunt aplicabile în cazul serviciilor de plată pe internet, indiferent de dispozitivul de acces utilizat. Serviciile cuprind: executarea plăților cu cardul pe internet, inclusiv plata cu carduri virtuale, precum și înregistrarea datelor de plată cu cardul pentru utilizarea în „soluții de tip portofel"; executarea transferurilor-credit pe internet; emiterea și modificarea mandatelor electronice de debitare directă; transferurile de bani electronici între două conturi de monedă electronică prin internet.

Principalele prevederi. Sunt 14 cerințe specifice, fiecare având un număr de sub-cerințe detaliate și o listă de 13 bune practici, care pot fi clasificate în două categorii, având în vedere următoarele: 1) măsuri specifice de control și de securitate pentru plățile pe internet și 2) conștientizarea din partea clientului, instruirea și comunicarea cu clienții.

1. Cerințe privind măsuri specifice de control și de securitate pentru plățile pe internet

Guvernanța. Prestatorii de servicii de plată trebuie să pună în aplicare și să revizuiască periodic o politică de securitate formală pentru serviciile de plată pe internet care trebuie să definească obiectivele de securitate și apetitul de risc. Potrivit bunelor practici, politica de securitate ar putea fi stabilită într-un document dedicat.

Evaluarea riscurilor. Prestatorii de servicii de plată trebuie să efectueze și să documenteze evaluări detaliate ale riscurilor în ceea ce privește securitatea plăților pe internet și a serviciilor conexe, atât înainte de inițierea serviciului (serviciilor) cât și ulterior.

Monitorizarea și raportarea incidentelor. Prestatorii de servicii de plată trebuie să asigure monitorizarea, procesarea și urmărirea coerentă și integrată a incidentelor de securitate, inclusiv a reclamațiilor clienților legate de securitate și de asemenea să stabilească o procedură pentru raportarea incidentelor majore legate de securitatea plăților, către autoritățile competente. Prestatorii de servicii de plată trebuie să asigure prin mijloace contractuale cooperare e-comercianților în cazul incidentelor majore legate de securitatea plăților,așa cum sunt acestea definite în Ghid.

Controlul și reducerea riscurilor. Prestatorii de servicii de plată trebuie să pună în aplicare măsuri de securitate care trebuie să includă mai multe linii de apărare, în conformitate cu politicile lor respective de securitate, în scopul de a reduce riscurile identificate și ar trebui să fie supuși periodic unui audit independent. Acest tip de măsuri de securitate sunt unele din cele mai importante aspecte asupra cărora Ghidul are impact, întrucât acestea vor afecta rețelele, datele de plată sensibile, externalizarea și tehnologia folosite de prestatorii de servicii de plată. Aceștia trebuie să se asigure că e-comercianții și orice alți prestatori externi să pună în aplicare același tip de măsuri.

Trasabilitatea. Prestatorii de servicii de plată trebuie să aibă procese care să asigure faptul că toate operațiunile (inclusiv fluxul procesului e-mandat) sunt urmărite în mod corespunzător. Bunele practici prevăd că prestatorii de servicii de plată le-ar putea solicita prin contract e-comercianților care stochează informații de plată să dispună de procese adecvate care să asigure trasabilitatea.

Informațiile și identificarea inițială a clientului. Clienții trebuie să fie identificați în mod corespunzător, în conformitate cu legislația europeană privind combaterea spălării banilor și trebuie să-și confirme disponibilitatea de a efectua plăți pe internet folosind serviciile înainte de a primi accesul la astfel de servicii. Potrivit bunelor practici, clientul ar putea semna un contract de servicii dedicat efectuarării operațiunilor de plată pe internet (în loc ca termenii să fie incluși într-un contract mai larg de servicii generale încheiat cu prestatorul de servicii de plată). De asemenea, clienților ar trebui să le fie oferite instrucțiuni clare și simple care să le explice responsabilitățile pentru utilizarea securizată a serviciului.

Autentificarea strictă a clientului. Prestatorii de servicii de plată trebuie să se asigure că inițierea plăților pe internet, precum și accesul la datele sensibile de plată sunt protejate prin autentificarea strictă a clientului, în conformitate cu definiția prevăzută în Ghid. Exemple de autentificare strictă a clientului pot include elemente care leagă autentificarea de o anumită sumă și un anumit beneficiar. Bunele practici prevăd că, din motive de comoditate pentru client, prestatorii de servicii de plată ar putea lua în considerare utilizarea unui singur instrument de autentificare strictă a clientului, pentru toate serviciile de plată pe internet.

Înscrierea pentru instrumente și/sau programe software de autentificare livrate clientului și furnizarea acestora. Prestatorii de servicii de plată trebuie să se asigure că înscrierea clientului pentru instrumente de autentificare și furnizarea inițială a acestor instrumente, necesare pentru a utiliza serviciul de plată pe internet și/sau livrarea programelor software pentru plată către clienți se efectuează într-un mod securizat.

Încercările de logare, expirarea sesiunii, valabilitatea autentificării. Prestatorii de servicii de plată trebuie să limiteze numărul de încercări de logare sau de autentificare, să definească reguli pentru expirarea sesiunilor serviciilor de plată pe internet și să stabilească limite de timp pentru validitatea autentificării.

Monitorizarea operațiunilor. Mecanismele de monitorizare a operațiunilor, care au scopul de a preveni, de a detecta și de a bloca operațiunile de plată frauduloase trebuie să fie rulate înainte de autorizația finală a prestatorului de servicii de plată. De asemenea, operațiunile suspecte sau cu risc ridicat trebuie să facă obiectul unei examinări specifice și al unei proceduri de evaluare. Trebuie să existe, de asemenea, mecanisme echivalente de monitorizare a securității și de autorizare pentru emiterea de e-mandate.

Protecția datelor de plată sensibile. Ghidul prevede, în mod clar, că datele de plată sensibile trebuie să fie protejate atunci când acestea sunt stocate, procesate sau transmise. În cazul în care e-comercianții procesează date de plată sensibile, acești prestatori de servicii de plată trebuie să le solicite prin contract e-comercianților să dispună de măsurile necesare pentru a proteja aceste date. În acest scop, potrivit bunelor practici, este de dorit ca e-comercianții care procesează date de plată sensibile să își instruiască în mod corespunzător personalul de gestionare a fraudelor și să actualizeze această instruire, în mod regulat, pentru a se asigura că instruirea rămâne relevantă pentru un mediu de securitate dinamic.

2. Ghidul cu privire la conștientizarea din partea clientului, instruirea și comunicarea cu clienții

Instruirea clientului și comunicarea cu clienții. Prestatorii de servicii de plată trebuie să ofere asistență și îndrumare clienților, după caz, în ceea ce privește utilizarea securizată a serviciilor de plată pe internet. Cel puțin un canal securizat pentru comunicarea continuă cu clienții în ceea ce privește utilizarea corectă și sigură a serviciului de plată pe internet ar trebui să fie disponibil. De asemenea, potrivit bunelor practici este de dorit ca prestatorii de servicii de plată prin acceptarea cardurilor să organizeze programe de instruire referitoare la prevenirea fraudei pentru e-comercianții lor.

Notificări, stabilirea de limite. Înainte de a-i oferi unui client serviciile de plată pe internet, prestatorii de servicii de plată trebuie să stabilească limite aplicabile acestor servicii (de exemplu, o sumă maximă pentru fiecare plată individuală sau o sumă cumulată pe o anumită perioadă de timp) și trebuie să își informeze clienții în consecință. Prestatorii de servicii de plată trebuie să le permită clienților să dezactiveze funcționalitatea de plată pe internet.

Accesul clienților la informații despre starea de inițiere și execuție a plății. Prestatorii de servicii de plată trebuie să le confirme clienților inițierea plății și să le ofere clienților în timp util informațiile necesare pentru a verifica dacă o operațiune de plată a fost inițiată și/sau executată în mod corect. Extrasele electronice detaliate trebuie să fie puse la dispoziție prin intermediul unui mediu sigur și de încredere. Canalele alternative, cum ar fi SMS, e-mail sau scrisoare nu sunt considerate un mediu sigur și de încredere și prin urmare, datele de plată sensibile nu trebuie să fie incluse în astfel de comunicări sau, în cazul în care sunt incluse, acestea trebuie să fie mascate.

Implementare. Autoritatea competenta română trebuie să notifice ABE dacă se conformează sau intenționează să se conformeze cu prezentul ghid sau să comunice motivele neconformării până la 5 mai 2015. În absența unei notificări până la acest termen, ABE va considera că autoritatea competentă nu respectă cerințele conținute de Ghid.

Dacă aveți întrebări cu privire la prevederile ghidului, vă rugăm să nu ezitați să ne contactați.

Andrei Burz-Pinzaru
Avocat
+40 21 207 52 05

Irina Albusel
Avocat
+40 21 207 54 26

Pentru mai multe informații, vă rugăm să ne contactați la Romania@deloittece.com sau să vizitați pagina web: www.deloitte.com/ro/tax-alerts