

За 2024 г. незабавните плащания blink бележат рекорден ръст от 102.14%. Това означава ли, че все повече клиенти се доверяват на услугата?

Стоилка Арсова (С.А.): Да, ръстът от над 100% категорично показва, че все повече потребители използват услугата blink. Това доверие се дължи не само на удобството и бързината на незабавните плащания, но и на добавената стойност, която предоставяме чрез иновативни функционалности - например blink P2P - мигновени преводи по мобилен номер, както и blink parking - решение за почасово паркиране чрез незабавно плащане. Предстои и разширяване с функционалности за електронна търговия, което допълнително ще засили интереса и ползваемостта. Услугата обхваща целия пазар - всички банки и лицензирани платежни институции участват в нея. Обръщаме изключително внимание на сигурността и управлението на риска. Схемата (Национална картова и платежна схема - НКПС) въведе стандартизирани правила не само по отношение на продуктите и технологичните спецификации, но и конкретни изисквания за управление на риска, които са задължителни за всички участници.

Албена Петкова (А.П.): БОРИКА като оператор на платежни системи осигурява 24/7 мониторинг в реално време на трансакциите, вкл. blink трансакциите. Това е в основата на доверието, което потребителите и партньорите ни оказват. Заедно с предлаганите от БОРИКА anti-fraud услуги, базирани на водещата платформа IBM Safer Payments, дружеството прилага задълбочена експертиза и интегриран подход за защита от финансови измами.

Защо е толкова важна превен-



БОРИКА - един хог пред измамниците с въвеждането на мощни anti-fraud механизми за превенция

Стоилка Арсова,
директор „Национална картова и платежна схема“, БОРИКА

Албена Петкова,
директор „Превенция на финансови измами“, БОРИКА

цията на финансови измами в контекста на навлизането на незабавните плащания?

А.П.: Незабавните плащания изискват незабавна сигурност. Докато трансакцията се случва в реално време, рискът също възниква мигновено. Това налага използването на усъвършенствани инструменти - автоматизирани системи, които засичат нетипично поведение още преди завършването на плащането. IBM Safer Payments като централен елемент на нашата защита използва модели на поведение и машинно самообучение, за да открива аномалии и блокира съмнителни трансакции в реално време - без

да нарушава потребителското изживяване.

Какви са основните заплахи и угрози измами, с които се сблъскват потребителите при дигитални плащания, включително и blink?

А.П.: Една от най-сериозните заплахи при дигиталните плащания в момента са т.нар. измами с угълномощни плащания (authorized push payment fraud). Това са случаи, в които клиентът сам нарежда плащането, но под въздействие на измамник - обикновено след като е бил подведен чрез социално инженерство, фишинг имейли, фалшиви SMS-и или обаждания от лица,

представящи се за институции, които внушават доверие. Честа практика са и измами, свързани с онлайн пазаруване, при които клиентите плащат за стоки или услуги, които никога не получават.

Особената уязвимост на незабавните плащания като blink се дължи именно на тяхната основна характеристика - незабавност. Средствата напускат клиентската сметка в реално време и веднъж изпратени, обикновено е много трудно да бъдат възстановени. Това прави услугата изключително привлекателна за измамници, които действат бързо и анонимно. Превенцията на такива измами

изисква многопластов подход. От една страна, е изключително важно да се повиши информираността на потребителите - как да разпознават рисковете и как да реагират при съмнение. От друга страна, доставчиците на платежни услуги трябва да прилагат високотехнологични решения за автоматизирана защита. Тези решения включват платформи, които анализират поведението на клиента в реално време, засичат нетипични действия и автоматично задействат контролни механизми - всичко това без да нарушават преживяването на потребителя или да забавят самото плащане. Използват се сложни алгоритми и модели за оценка на риска, които сработват още по време на влизане в мобилното банкиране или онлайн платформата, при въвеждане на плащане и по време на целия процес.

Важно е да се подчертае, че превенцията не се свежда до еднократна проверка. Това е система от множество взаимосвързани и адаптивни риск контроли, които работят във фонов режим - незабележимо за потребителя, но с висока ефективност за спиране на измамни опити в реално време.

Какви конкретни мерки сте въвели за превенция на измами при blink?

С.А.: НКПС има разработени правила за оценка на риска, които използват данни, предавани чрез съобщения в системата. Всички институции са свързани с БОРИКА чрез интерфейси и обменят информация, която позволява изграждането на механизми за разпознаване на потенциални измамни схеми. Целта ни е, ако даден клиент бъде атакуван в една банка, да можем да го идентифицираме и в друга - и да реагираме навреме. Скоростта е критична.

Как си сътрудничите с доставчиците на платежни услуги за обезпечаване сигурността на клиентите им?

С.А.: В рамките на Схемата сме изградили структурирана



Все повече потребители използват услугата blink.

Стоилка Арсова



Незабавните плащания изискват незабавна сигурност.

Албена Петкова

Сигурността на blink е заложена още в основата на потребителския интерфейс. Например при услугата blink P2P (превод по мобилен номер) - клиентът вижда още преди потвърждение на плащането както името на получателя от контактната му листа, така и официалното име, на което е банковата сметка. Това създава възможност за моментална проверка и информирано решение дали да се продължи с плащането.

А.П.: Ние надграждаме тези технологични защити с интегрирани решения за управление на риска. Разработваме цялостна рамка, която обхваща всички продукти, използвани от клиента - така можем да анализираме какво поведение е типично или нетипично за даден клиент или за определен пазарен сегмент. Това включва например времето на плащане, вида на търговеца или честота на трансакции.

На тази база създаваме автоматизирани риск контроли, които работят в реално време. Това означава, че мерките за защита се задействат още преди завършването на трансакцията. Само така можем да сме ефективни - чрез автоматизация, която идентифицира заплахи и реагира мигновено, без да нарушава потребителското изживяване.

Как си сътрудничите с доставчиците на платежни услуги за обезпечаване сигурността на клиентите им?

С.А.: В рамките на Схемата сме изградили структурирана

мрежа от работни групи, в които участват над 200 експерти от всички лицензирани доставчици на платежни услуги в България. Тези групи функционират като платформа за редовен обмен на информация и съгласуване на правила, свързани с управлението на риска и сигурността на клиентите. Виждаме себе си като свързващо звено между участниците, което улеснява координацията и сътрудничеството. Непрекъснато обменяме опит и с наши международни партньори по отношение на адаптирането ни към новите предизвикателства в областта на сигурността на плащанията.

А.П.: Наред с това с всеки от клиентите си БОРИКА изгражда индивидуален подход - анализираме техния потребителски профил и разработваме специфични anti-fraud механизми. Целта е баланс между ефективна защита и високо ниво на успешно обработени трансакции. Това включва анализ на типичното и нетипичното поведение на потребителите, обемите на трансакциите и други релевантни фактори. Целта е да разработим интелигентни и ефективни решения за управление на риска, които да минимизират измамните, като същевременно максимизират успешните трансакции и поддържат високо ниво на клиентско удовлетворение.

Какво га очакваме в бъдеще в сферата на сигурните плащания?

А.П.: В бъдеще ще виждаме

още по-умни и усъвършенствани технологии за превенция на измами. Както измамниците използват все по-сложни методи, така и ние трябва да отговаряме с най-модерните инструменти - включително решения, базирани на изкуствен интелект и машинно самообучение. Целта е да сме винаги една крачка пред тях - чрез автоматизирани системи, които в реално време идентифицират и блокират съмнителни трансакции. Същевременно ще работим за това клиентите да имат още по-сигурен, лесен и доверен достъп до дигиталните разплащателни канали.

С.А.: Регулаторната рамка на Европейския съюз и SEPA също се развива в посока на по-стриктен мониторинг на незабавните плащания. Една от ключовите мерки е въвеждането на задължителна верификация на получателя - функция, която ще адаптираме хармонизирано със SEPA Instant Payments. Освен за незабавните плащания БОРИКА като оператор ще разшири тази услуга и към други видове кредитни трансфери. Това ще дава възможност при въвеждане на данни за получателя - име, IBAN или мобилен номер - системата да връща обратна информация дали има съвпадение, което ще даде възможност на подателя да потвърди или откаже плащането. Това вече е уредено за blink P2P. Очаква се тази мярка значително да намали риска от измами. С фокус върху електронната търговия ще засилим не само мерките за превенция на измами, но и възможностите за справедливо разрешаване на оспорени плащания. Това е от ключово значение за клиентската удовлетвореност - ще въведем ясни правила, които да позволят на потребителите бързо да възстановят средствата си при доказани нередности или некоректни търговци.