Bezpieczny handel w internecie

Pierwsze badanie zjawiska oszustw płatniczych w polskim e-commerce

Nethone

EY
Building a better working world

Spis treści

Szanowni Państwo,

z wieloletniego doświadczenia w doradzaniu firmom w zakresie przeciwdziałania nadużyciom wiemy, że w polskich realiach tematyka ta zazwyczaj nie jest wysoko na liście ich priorytetów. Zazwyczaj zmienia się to dopiero w momencie, kiedy na skutek nadużyć firma ponosi znaczne straty finansowe lub wizerunkowe. Obserwujemy też, że do tej pory w Polsce tylko nieliczne branże próbują w sposób systematyczny i zorganizowany zarządzać ryzykiem nadużyć. Do tej grupy należą oczywiście instytucje finansowe, w których zapobieganie wyłudzeniom to nieodłączna część biznesu.

Z tym większym zainteresowaniem przyjęliśmy propozycję przeprowadzenia wspólnie z Nethone pierwszego w Polsce badania zjawiska oszustw płatniczych w polskim e-commerce. Branża ta dynamicznie się rozwija i coraz częściej możemy zaobserwować polskie firmy, które śmiało wchodzą na zagraniczne rynki. Im większy zasięg sklepu i skala działalności, tym ryzyko jest większe. Naszym zdaniem, warto przyjrzeć się bliżej zagrożeniom związanym z fraudem płatniczym oraz zawczasu podjąć działania, które pozwolą w sposób bezpieczny kontynuować rozwój, a być może nawet osiągnąć przewagę nad konkurencją.

Życzę miłej lektury!

Marcin Bizoń

Associate Partner

Dział Zarządzania Ryzykiem Nadużyć

EY Polska

Szanowni Państwo,

świat handlu online rozwija się w zawrotnym tempie, wkraczając w coraz to nowe obszary. Od dłuższego czasu obserwujemy jak firmy prowadzące sprzedaż towarów i usług w internecie rosną w siłę, jak gracze o ugruntowanej pozycji w świecie handlu tradycyjnego uruchamiają kanały sprzedaży online, jak konsumenci zmieniają swoje preferencje i poszukując najlepszych ofert, coraz częściej kierują się do sieci. Niestety tam, gdzie pojawiają się duże pieniądze, działać zaczynają przestępcy. Zjawisko tzw. fraudu płatniczego jest dziś często określane mianem jednego z najpoważniejszych wyzwań dla światowego e-commerce. Będąc polską firmą działającą globalnie, postanowiliśmy przyjrzeć się problemowi na rodzimym rynku. Poszukując wiarygodnych danych odkryliśmy, że nikt dotąd nie badał specyfiki fraudu płatniczego w Polsce, a przynajmniej nie ukazało się tu jeszcze żadne przekrojowe opracowanie na ten temat. Właśnie dlatego, wspólnie z EY, przeprowadziliśmy badanie ankietowe na próbie 150 firm handlujących w internecie, a jego rezultaty i nasze wnioski zawarliśmy w niniejszym opracowaniu. Mam nadzieję, że będzie ono dla Państwa wartościowym źródłem informacji, a zarazem przestrogą przed bagatelizowaniem problemu.

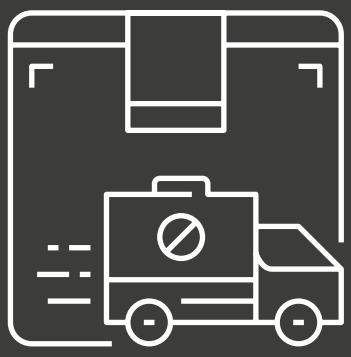
Zapraszam do lektury!

Hubert Rachwalski

CEO

Nethone

Fraud płatniczy - na czym polega i dlaczego jest groźny dla biznesu e-commerce?



Fraud płatniczy, czyli nadużycie polegające na oszustwie przy płatnościach, jest często określany mianem jednego z najpoważniejszych zagrożeń, z jakim mierzyć się muszą dziś firmy handlujące online. Na czym polega? W największym uproszczeniu, do fraudu dochodzi wówczas, gdy płatności za towary czy usługi dokonuje osoba do tego nieuprawniona. W praktyce chodzi na ogół o transakcję dokonywaną przez oszusta w Internecie za pomocą kradzionej karty płatniczej, a właściwie kradzionych danych karty: jej numeru, imienia i nazwiska posiadacza, daty ważności i kodu zabezpieczającego (tzw. CVC/CVV). Niemal codziennie media donoszą o wyciekach danych z baz różnego rodzaju organizacji – w tym dużych sklepów internetowych czy instytucji finansowych. Według szacunków firmy Gemalto, co minutę na świecie „wycieka" z baz niemal 3,5 tys. rekordów[1]. Często są to właśnie dane kart płatniczych bądź loginy i hasła użytkowników służące do logowania w różnego rodzaju serwisach – nieraz umożliwiających dokonywanie zakupów. Ponadto, posiadacze kart nieraz padają ofiarą tzw. skimmingu, czyli przechwytywania danych kart płatniczych za pomocą specjalnych urządzeń zakładanych przez przestępców na bankomaty czy terminale POS. Na całym świecie działają doskonale zorganizowane grupy przestępcze wyspecjalizowane w wykradaniu danych i sprzedawaniu ich na czarnym rynku. W 2016 roku firma Equifax alarmowała, że średnia czarnorynkowa cena działającej karty z USA wynosiła zaledwie ok. 13,6 USD[2]. Przestępcy zajmujący się wyłudzeniami (tzw. fraudsterzy) kupują kradzione dane kartowe na czarnym rynku, a następnie masowo dokonują za ich pomocą zakupów w sieci. Proces jest często zautomatyzowany. Oszuści wykorzystują m.in. boty zdolne samodzielnie odwiedzić sklep internetowy, skompletować koszyk i opłacić zakupy przy użyciu kradzionych danych kartowych.

Kiedy prawowity posiadacz karty odkrywa, że została ona obciążona z tytułu transakcji, których nie dokonywał, zwykle kontaktuje się ze swoim bankiem – wydawcą karty – i inicjuje procedurę reklamacji. Jej skutkiem jest najczęściej tzw. obciążenie zwrotne (chargeback), czyli zwrot bezprawnie pobranych środków.

Ponieważ w całym ekosystemie płatniczym najlepiej chronionym podmiotem jest konsument, obowiązek zwrotu pieniędzy oraz pokrycia większości kosztów związanych z procedurą spoczywa niemal w całości na sprzedającym, który zaakceptował nieuprawnioną transakcję.

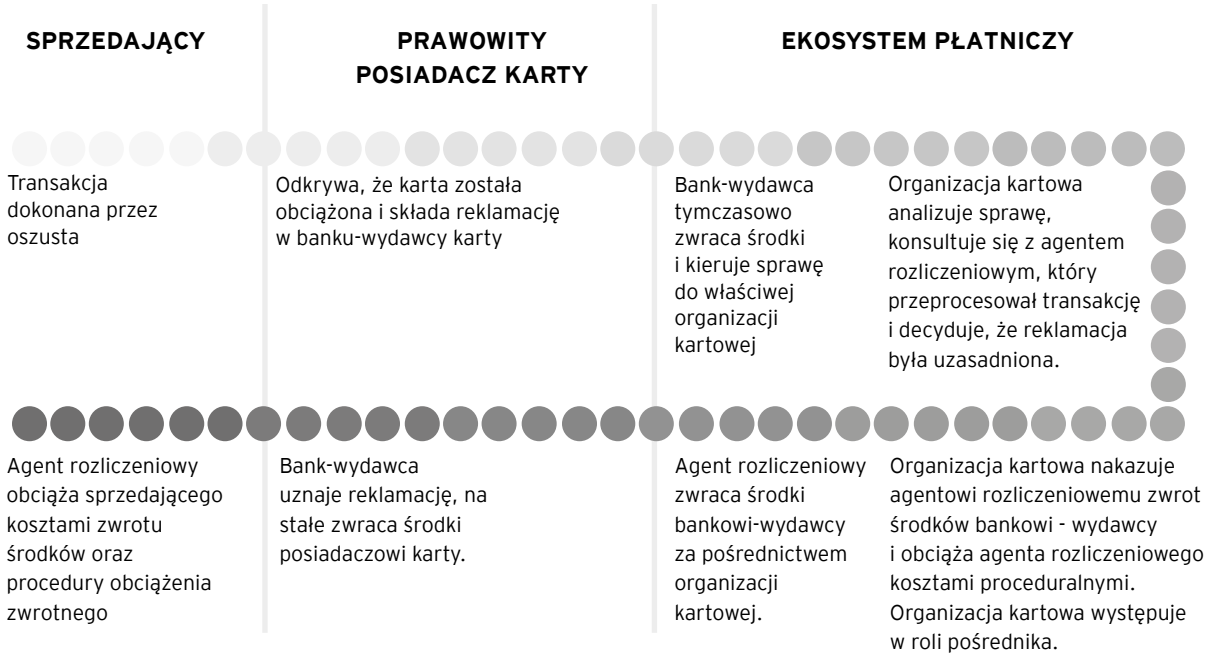
W efekcie traci on towar, który został wysłany oszustowi, traci pieniądze, które musi zwrócić prawowitemu posiadaczowi karty i dodatkowo ponosi koszty proceduralne – nieraz przewyższające wartość samej feralnej transakcji. Choć z formalnego punktu widzenia zwrot środków oraz obowiązek pokrycia kosztów operacyjnych leżą w znacznej mierze

1 http://breachlevelindex.com/

2 https://fossbytes.com/infographic-dark-web-stolen-credit-card-price/

po stronie podmiotu procesującego płatność – a zatem agenta rozliczeniowego – regulaminy tego typu instytucji na ogół zakładają przeniesienie tej odpowiedzialności na akceptantów, czyli sprzedawców.

Chargeback. Jak to działa?



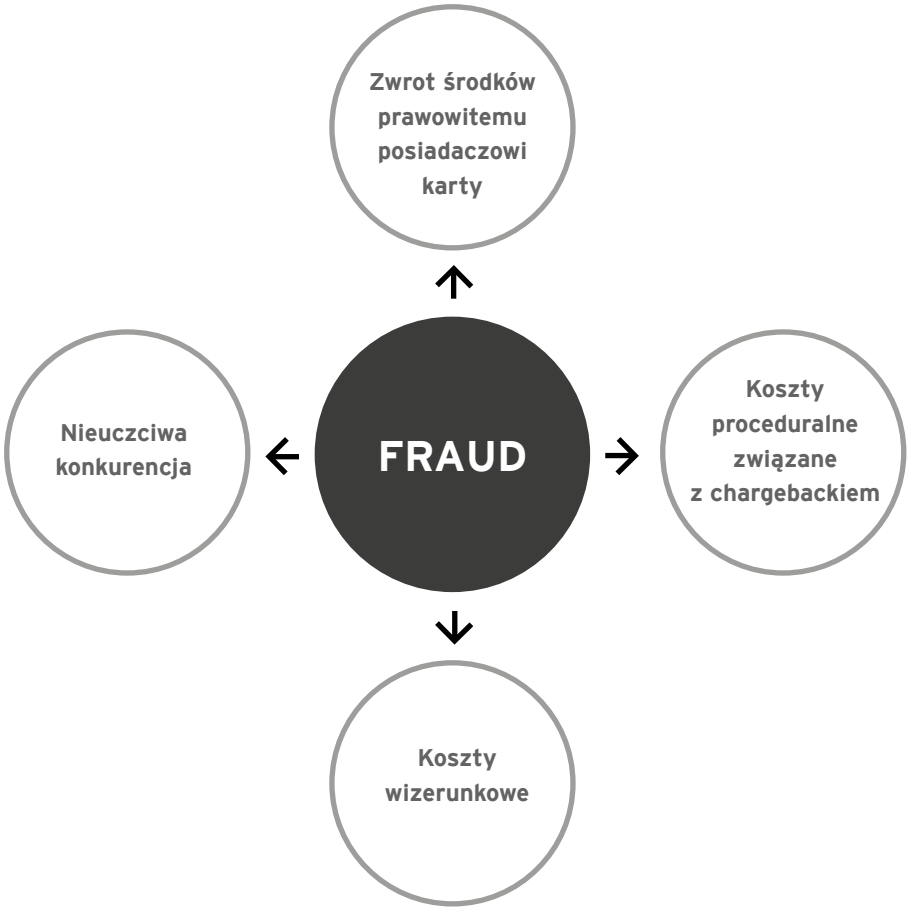
Aby chronić konsumentów przed sprzedawcami, którzy nie są w stanie skutecznie zadbać o bezpieczeństwo konsumentów, organizacje kartowe wprowadziły limity dopuszczalnych liczb i wartości fraudów notowanych miesięcznie przez akceptantów. Limity dotyczą zarówno sprzedawców online, jak i agentów rozliczeniowych. Ich przekroczenie w najlepszym wypadku wiąże się z karami finansowymi, wzrostem kosztów procesowania transakcji i koniecznością wprowadzenia lepszych zabezpieczeń, w najgorszym – z utratą możliwości dalszego akceptowania kart głównych organizacji, co w przypadku e-commerce na ogół jest równoznaczne z końcem biznesu.

Monitorowanie sytuacji firmy w kontekście fraudu płatniczego samo w sobie nie jest łatwym zadaniem. Ponieważ procedura rozpatrywania reklamacji wymaga czasu, sprzedawca, który pada ofiarą oszustów, niejednokrotnie dowiaduje się o tym z wielotygodniowym opóźnieniem – gdy otrzymuje od swojego agenta rozliczeniowego raport o wymagających uregulowania chargebackach.

W efekcie, firma może przez dłuższy czas funkcjonować w przekonaniu, że z powodzeniem zwiększa sprzedaż, podczas gdy w istocie jest wręcz odwrotnie.

Konsekwencje fraudu płatniczego w rzeczywistości wykraczają daleko poza obszar finansów. Fraud płatniczy trwale niszczy reputację firm padających jego ofiarą. Konsument, którego kartą w nieuprawniony sposób zapłacono w danym sklepie, najprawdopodobniej nigdy sam nie zrobi w nim zakupów i będzie odradzał to innym. Informacja o tym, że dane przedsiębiorstwo nie radzi sobie najlepiej z zabezpieczaniem się przed oszustami może skutecznie odstraszyć zarówno kupujących, jak i inwestorów. Ponieważ wyłudzone towary szybko trafiają do obrotu na rynku wtórym, a ich ceny są tam z reguły znacznie niższe niż w regularnych e-sklepach, biznes musi mierzyć się dodatkowo z nieuczciwą konkurencją. Jest to szczególnie odczuwalne w takich branżach, jak dobra cyfrowe czy towary luksusowe.

Wpływ oszustw kartowych na przedsiębiorcę przyjmującego płatność



Fraud płatniczy na świecie

Jak zauważono na początku niniejszego rozdziału, fraud płatniczy uważany jest za jedno z najpoważniejszych zagrożeń dla współczesnego e-commerce. Aby choć częściowo unaocznić skalę problemu, wystarczy odwołać się do raportów sektorowych. W 2016 roku magazyn branży płatniczej The Nilson Report prognozował, że globalne straty ponoszone z powodu fraudu przez różnego rodzaju podmioty, w tym sprzedawców, banki i organizacje kartowe, osiągną w 2019 roku wartość blisko 33 mld USD.[3] Tymczasem, zaledwie rok po opublikowaniu prognozy, autorzy serwisu PYMNTS.com, tworzący cykliczne opracowanie na temat skali problemu fraudowego na świecie – The Global Fraud Index – szacowali, że w pierwszym kwartale 2017 roku łączna wartość strat będących wynikiem fraudu wyniosła aż 57,8 mld USD – niemal dwukrotnie więcej. Warto zauważyć, że ich szacunki odnosiły się wyłącznie do strat poniesionych przez podmioty działające w ośmiu, wybranych na potrzeby raportu, branżach.[4] Z tego samego źródła wynika, że liczba fraudów płatniczych rośnie w tempie ok. 5,5% w skali roku, przy czym w niektórych segmentach e-commerce stopa wzrostu jest znacznie wyższa. Przykładowo, w segmencie kosmetyczno -perfumeryjnym wyniosła w analizowanym okresie ponad 171%.[5] Jeśli chodzi o statystyki dla Europy, ostatnie oficjalne opracowanie na temat fraudu kartowego przygotowane przez Europejski Bank Centralny pochodzi z 2015 roku i bazuje na danych z 2013 roku, a zatem – biorąc pod uwagę tempo, w jakim zmienia się świat handlu online – dawno przestało być aktualne. Należy jednak zauważyć, że już w latach 2011-2013 w odniesieniu do liczby i wartości fraudów kartowych obserwowano wyraźną tendencję wzrostową.[6] Warto zatem odnieść się do nowszych danych - przytaczanych przez firmę

3 https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf

4 Używki, elektronika użytkowa, kosmetyki i perfumy, domy towarowe, meble i wyposażenie domu, zdrowie, rekreacja i hobby, biżuteria i metale szlachetne https://www.pymnts.com/download-global-fraud-index-october-2017/

5 Ibid.

6 https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

FICO na bazie Euromonitora. Wynika z nich, że w 2016 roku straty spowodowane przez fraud w regionie EMEA (Bliski Wschód, Europa Afryka) wyniosły prawie 1 mld EUR. Według tego samego źródła, wartość strat spowodowanych przez fraud w Polsce wynosiła w 2016 roku ponad 35 mln PLN. Choć w porównaniu z wartościami globalnymi, kwota ta może wydawać się ledwo zauważalna, warto mieć na uwadze, że Polska uplasowała się na drugim miejscu (po Szwecji) pod względem wysokości rocznej stopy przyrostu wartości strat wynikających z fraudu kartowego (10% YoY)[7]. Innymi słowy, skala problemu – choć lokalnie stosunkowo niewielka – szybko rośnie. Co prawda różnorodność metod obliczeń stosowanych przez autorów różnych opracowań nie pozwala bezpośrednio porównywać rezultatów, jednak wszystkie przytoczone statystyki dowodzą, że problemu fraudu płatniczego nie wolno ignorować – w szczególności, jeśli prowadzi się biznes adresujący ofertę do konsumentów z całego świata, a możliwość takiego właśnie działania jest przecież jednym z największych atutów handlu internetowego.

Z gwałtownym przyrostem liczby fraudów w Internecie światowy biznes ma do czynienia od października 2015 roku. Wówczas to w Stanach Zjednoczonych weszły w życie regulacje ustanowione przez główne organizacje kartowe w odniesieniu do odpowiedzialności za wyłudzenia w handlu stacjonarnym dokonywane z użyciem kart bez chipa (głównie bazujące na paskach magnetycznych). W USA zabezpieczanie karty chipem oraz kodem PIN jest nowością. Polskiemu czytelnikowi zagadnienie może wydać się nieco egzotyczne, ponieważ od wielu lat nad Wisłą emituje się niemal wyłącznie karty wyposażone w chip, a co za tym idzie – wszędzie tam, gdzie można płacić kartą, terminale POS są przystosowane do współpracy tego rodzaju narzędziami płatniczymi. Ponieważ jednak przyjmowanie płatności kartowych ma za oceanem znacznie dłuższą tradycję niż w Europie, przez wiele lat nie wprowadzano tam innowacyjnych zabezpieczeń ze względu na wiążące się z tym koszty infrastrukturalne wynikające ze skali takiej akcji modernizacyjnej – z rozległości i gęstości sieci akceptacji oraz liczby kart w użyciu. Co uległo zmianie przed trzema laty? Krótko mówiąc, od października 2015 roku to amerykański sprzedawca ponosi odpowiedzialność finansową za każde wyłudzenie, które nastąpiło w handlu stacjonarnym z wykorzystaniem karty wyposażonej wyłącznie w pasek magnetyczny i/lub tłoczony numer. Regulacje wprowadzono ze względów bezpieczeństwa – aby niejako wymusić na akceptantach i agentach rozliczeniowych modernizację i położyć kres fałszerstwu kart. Karty z chipem są znacznie trudniejsze do podrobienia niż tradycyjne „plastiki". Co oczywiste, wiązało się to z istotnymi kosztami po stronie biznesu – w szczególności wymiany wymagały terminale płatnicze. Manewr ten przyniósł oczekiwane rezultaty w postaci znacznego zmniejszenia liczby wyłudzeń z wykorzystaniem podrabianych kart w fizycznych punktach sprzedaży. Niestety, wywołał również nieoczekiwane konsekwencje – mianowicie skupienie uwagi oszustów na handlu internetowym, gdzie do dokonania wyłudzenia nie trzeba fałszować karty i wykradać kodu PIN – wystarczy wejść w posiadanie informacji widniejących na samej karcie. Oszuści przenieśli się więc do Internetu, a rozwój zorganizowanej przestępczości finansowej online na terenie USA przełożył się na sytuację globalną.

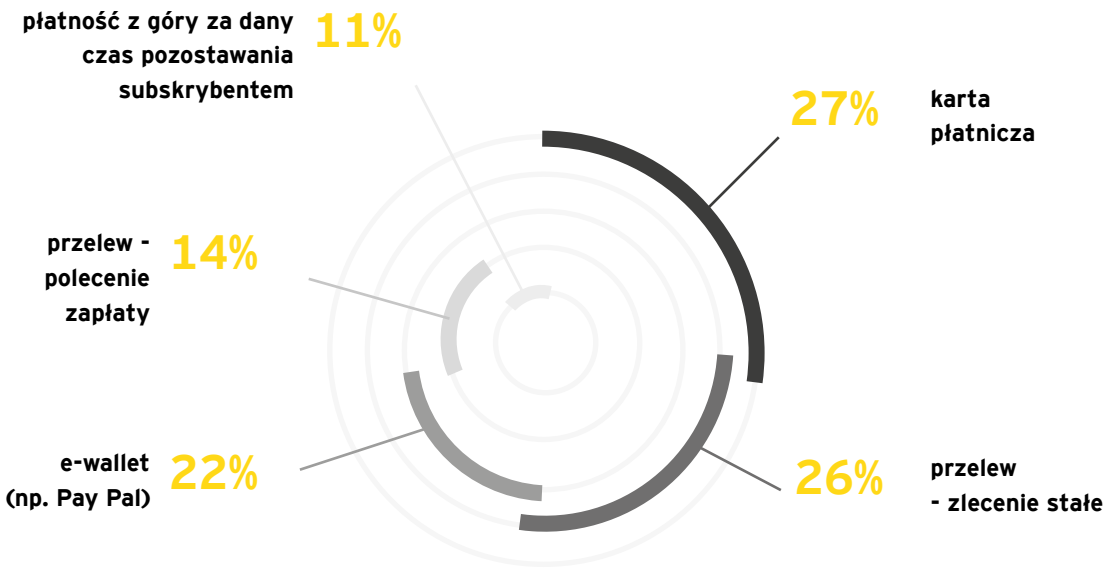
7 http://www.fico.com/europeanfraud/poland

Fraud płatniczy w Polsce

Pomimo opisanej powyżej skali zjawiska, pojęcie fraudu płatniczego może dla polskiego czytelnika być zupełnie nowym. Wynika to przede wszystkim ze specyficznej struktury polskiego rynku e-commerce pod względem wykorzystywanych i preferowanych przez tutejszych konsumentów metod płatności. Jak wyjaśniono powyżej, do fraudu najczęściej dochodzi w związku z transakcjami dokonywanymi za pomocą kart płatniczych w Internecie. Tymczasem, inaczej niż na większości rynków, w Polsce karty płatnicze nie są najczęściej wybieraną metodą płatności online. Dominują tu tzw. szybkie przelewy pay-by-link oraz płatności za pobraniem. Tym niemniej, widoczny jest stopniowy wzrost popularności internetowych płatności kartowych – wynikający głównie z wkraczania na polski rynek usług bazujących na kartach. Mowa w szczególności o biznesach działających w modelu subskrypcyjnym, gdzie zapisane w systemie dane karty płatniczej są wykorzystywane przez sprzedającego do automatycznego pobierania płatności na podstawie określonego planu (np. dostęp do VoD czy streamingu muzyki) lub też bieżącego zużycia (np. usługi telekomunikacyjne czy transportowe). Według danych firmy Straal – dostawcy rozwiązań płatniczych posiadającego bogatą ofertę dla biznesu subskrypcyjnego – aż 27% polskich konsumentów do opłacania subskrypcji wybiera kartę płatniczą lub e-wallet wykorzystujący kartę.

Warto zwrócić również uwagę na zjawisko międzynarodowej ekspansji polskich firm przyjmujących płatności online. W Polsce działa coraz więcej firm, które swoje produkty lub usługi wytwarzają/świadczą na terytorium naszego kraju, lecz dostarczają je głównie klientom z zagranicy. Mowa w szczególności o firmach z rynku cyfrowego – dostawcach oprogramowania, wydawcach gier itd. Takie firmy muszą obowiązkowo przyjmować płatności kartowe i liczyć się z ryzykiem wystąpienia fraudu płatniczego.

Najczęściej wybierane metody płatności za subskrypcje



Fraud płatniczy w różnych sektorach e-commerce

Chociaż sama mechanika fraudu płatniczego jest we wszystkich segmentach handlu online podobna, specyfika zjawiska - a zatem to, co motywuje oszustów i implikuje bezpośrednio sposób ich działania - zasadniczo różni się w poszczególnych obszarach rynku. Wyróżnić można tu 4 podstawowe czynniki determinujące naturę fraudu płatniczego w różnych sektorach e-commerce. Są to: 1) forma przedmiotu transakcji – cyfrowa lub fizyczna, 2) stosunek średniej wartości pojedynczej transakcji do średniej liczby transakcji dokonywanych przez kupujących w określonej jednostce czasu, 3) średnia częstotliwość zakupów dokonywanych przez pojedynczego kupującego u danego sprzedawcy, 4) trudność lub łatwość zbycia dóbr na rynku wtórnym. Przez pryzmat powyższych dokonano krótkiej charakterystyki specyfiki problemu fraudowego w wybranych, szczególnie narażonych na wyłudzenia, branżach.

Dobra i usługi cyfrowe

Forma przedmiotu transakcji:	Średnia wartość pojedynczej transakcji:	Liczba transakcji dokonywanych w czasie:	Częstotliwość dokonywanych transakcji:	Rynek wtórny:
cyfrowa	**niska**	**wysoka**	**wysoka**	**duży**

Szeroko rozumiana branża dóbr i usług cyfrowych jest zdecydowanie najbardziej podatna na fraud płatniczy. Wynika to przede wszystkim z tego, że realizacja zamówienia odbywa się w całości drogą elektroniczną i ma miejsce w ciągu kilku do kilkunastu sekund od transakcji. W efekcie, nie ma tu czasu na weryfikację adresu dostawy czy możliwości sprawdzenia tożsamości odbiorcy zamówienia podczas fizycznego z nim kontaktu w momencie przekazania przesyłki. Średnia wartość pojedynczej transakcji jest w segmencie dóbr cyfrowych stosunkowo niska, zaś liczba transakcji dokonywanych w niemal dowolnej jednostce czasu – wysoka. Powyższe warunki sprzyjają automatyzacji wyłudzeń poprzez wykorzystywanie botów i umasowienie transakcji. Ponadto, dobra cyfrowe bardzo łatwo zbyć na rynku wtórnym – nie tracą one swoich walorów wraz z pierwotnym zakupem, a w sieci dostępna jest bogata oferta rozwiązań ułatwiających obrót nimi.

Gry komputerowe

Forma przedmiotu transakcji:	Średnia wartość pojedynczej transakcji:	Liczba transakcji dokonywanych w czasie:	Częstotliwość dokonywanych transakcji:	Rynek wtórny:
cyfrowa	**niska**	**bardzo wysoka**	**bardzo wysoka**	**bardzo duży**

Rynek gier komputerowych przynależy co prawda do szeroko rozumianego e-commerce dóbr i usług cyfrowych, jednak ze względu na swoją szczególną podatność na fraud został opisany jako oddzielna kategoria. W ramach rynku gier mówić można zarówno o obrocie kluczami licencyjnymi, tj. kodami umożliwiającymi pobieranie i użytkowanie oprogramowania bez konieczności posiadania trwałego nośnika, jak również o ogromnym rynku różnego rodzaju artefaktów, dodatków i modyfikacji do gier. Obrót handlowy realizowany jest zarówno za pośrednictwem platform certyfikowanych przez wydawców gier, jak i za pomocą niezależnych serwisów i forów. Średnia wartość pojedynczej transakcji jest tu niska, choć zdarzają się przypadki bardzo rzadkich artefaktów, których cena sięga nawet kilku tysięcy dolarów. Większość operacji dotyczy jednak dokonywanych wielokrotnie przez pojedynczego użytkownika zakupów o wartości od kilku do kilkunastu dolarów. Liczba transakcji dokonywanych w czasie jest tu bardzo wysoka. Sprzyja to automatyzacji wyłudzeń. Oszuści często wspomagają się botami, które wykonują setki transakcji, testując tym samym różne karty płatnicze. Niska wartość transakcji powoduje, że oszustwo jest stosunkowo trudno wykryć. Prawowici posiadacze kart, zwłaszcza tacy, którzy sami często robią zakupy przez Internet lub grają w gry sieciowe nieraz zauważają, że ich rachunek został obciążony za sprawą wyłudzenia na długo po tym, jak doszło do transakcji lub dopiero wówczas, gdy ich karta zostanie wykorzystana przez oszustów wielokrotnie. Automatyzacja fraudu powoduje również, że sprzedawcy łatwo mogą przekroczyć wspomniane wcześniej progi chargebackowe ustanawiane przez organizacje kartowe. Fraud płatniczy w branży gier często występuje w połączeniu z innymi formami wyłudzeń. Przykładowo, na porządku dziennym jest w tym obszarze e-commerce przejmowanie kont czy stosowanie e-dopingu pod różnymi postaciami.

Podróże

Forma przedmiotu transakcji:	Średnia wartość pojedynczej transakcji:	Liczba transakcji dokonywanych w czasie:	Częstotliwość dokonywanych transakcji:	Rynek wtórny:
cyfrowa/fizyczna	**wysoka**	**średnia**	**średnia**	**znikomy**

Branża usług zawiązanych z podróżami od lat cierpi z powodu fraudu płatniczego. Do tej kategorii zaliczają się wszystkie podmioty uczestniczące w procesie rezerwacji i realizacji usług powiązanych z mobilnością i zakwaterowaniem. Znajdziemy tu więc zarówno linie lotnicze, jak i internetowe biura podróży, metawyszukiwarki, systemy rezerwacji biletów lotniczych, kolejowych czy autobusowych, a także wypożyczalnie samochodów, hotele, pensjonaty, serwisy pośredniczące w krótkoterminowym wynajmie nieruchomości itd. W segmencie „travel" przedmiotem transakcji jest zwykle przekazywane w formie cyfrowej zobowiązanie sprzedawcy do wykonania określonej usługi w formie fizycznej. Przykładowo, bilet lotniczy sprzedawany w formie cyfrowej jest zobowiązaniem przewoźnika do wykonania usługi transportowej na określonych warunkach. Choć transakcji dokonuje się tu znacznie mniej niż w przypadku choćby rynku gier, opiewają one na znacznie wyższe kwoty – od kilkudziesięciu do kilku tysięcy dolarów. Jeśli zaś chodzi o rynek wtórny, działa on bardzo sprawnie. Odsprzedanie biletu lotniczego w praktyce opiera się na przekazaniu numeru rezerwacji i zmianie danych pasażera w systemie linii lotniczej czy internetowego pośrednika. Co więcej, ofiarą wyłudzeń w tym segmencie e-commerce padają nie tylko sprzedawcy i posiadacze kart, ale również osoby kupujące bilety od oszustów. Otrzymują one często bilety wygenerowane przed tym, jak linia lotnicza wykryje wyłudzenie i anuluje transakcję. W efekcie, takie bilety są bezwartościowe, zaś w wypadku, gdy oszukany kupujący dokonał płatności za trefne zakupy za pomocą karty, jego dane niemal na pewno posłużą oszustom do kolejnych wyłudzeń. Wykrycie fraudu jest w biznesie turystycznym szczególnie trudne. Zakupy dokonywane są przez osoby z całego świata, za pomocą wielu różnych rodzajów kart, a sytuacje nietypowe w innych segmentach e-commerce są tu na porządku dziennym. Przykładowo, fakt, że klient z Warszawy kupuje bilet z Meksyku do Chile nie jest niczym dziwnym. Być może właśnie planuje swoją podróż po Ameryce Łacińskiej? W handlu detalicznym, gdyby klient z Warszawy kupował w meksykańskim sklepie np. smartfon, podając jako adres dostawy lokalizację w Peru, najprawdopodobniej wzbudziłoby to wątpliwości meksykańskiego sklepu co do legalności transakcji.

Dobra luksusowe

Forma przedmiotu transakcji:	Średnia wartość pojedynczej transakcji:	Liczba transakcji dokonywanych w czasie:	Częstotliwość dokonywanych transakcji:	Rynek wtórny:
fizyczna	**bardzo wysoka**	**niska**	**niska**	**bardzo duży**

Ponieważ nic tak nie przyciąga oszustów jak wysoka wartość dóbr, które mogą wyłudzić, na ich celownik trafiają bardzo często sklepy internetowe handlujące towarami luksusowymi. Takie okoliczności pozwalają wyłudzić większe pieniądze przy mniejszej liczbie prób. Wartość pojedynczej transakcji jest w tym segmencie bardzo wysoka, a wolumeny transakcyjne są stosunkowo niskie. Klienci nie powracają do sklepu zbyt często. Towary luksusowe konsumenci kupują raczej okazjonalnie. Zbycie wyłudzonych dóbr na rynku wtórnym jest natomiast nawet łatwiejsze niż w przypadku dóbr cyfrowych. Z uwagi na wysokie ceny detaliczne na rynku pierwotnym, konsumenci bardzo często poszukują oryginalnych produktów w serwisach z ogłoszeniami czy na platformach handlowych. W efekcie, sprzedawcy dóbr luksusowych muszą dodatkowo rywalizować z bardzo silną, często nieuczciwą konkurencją. Wysoka wartość transakcji powoduje, że oszuści podejmują znacznie większy niż w przypadku,v np. dóbr cyfrowych wysiłek, aby wyłudzenie zakończyło się powodzeniem. Niejednokrotnie przestępcy zbierają mnóstwo informacji na temat prawdziwego posiadacza karty, wnikliwie je analizują i dokładają ogromnych starań, by w sieci upodobnić się do niego w stopniu uniemożliwiającym wykrycie wyłudzenia. Przykładowo, rejestrując konto w sklepie internetowym podają numer telefonu z prefiksem kierunkowym takim samym, jak w przypadku prawowitego posiadacza karty. Przeglądają jego profile w serwisach społecznościowych, wyciągając informacje, które mogą się przydać do uwiarygodnienia legendy w razie weryfikacji – znają imiona partnerów, dzieci i zwierząt ofiary, znają daty urodzin ważnych dla nich osób, czy terminy, w jakich ci przebywali na wakacjach za granicą. Te informacje są często publicznie dostępne. Ponieważ w niektórych przypadkach, jeśli regulamin sklepu na to pozwala, sprzedawca ma prawo poprosić kupującego o potwierdzenie tożsamości poprzez przesłanie skanu dokumentu tożsamości, oszuści potrafią uciekać się do fałszowania takich dokumentów. Są więc świetnie przygotowani. Z perspektywy sprzedawcy, to tylko jedna strona problemu. Drugą, równie ważną, jest łatwość, z jaką handlując towarami luksusowymi może przekroczyć wspomniane wcześniej progi chargebackowe ustanawiane przez organizacje kartowe. Przy wysokokwotowych transakcjach

czasem wystarczy zaledwie kilka chargebacków, by zostać uznanym za sprzedawcę wysokiego ryzyka i zmierzyć się z groźbą utraty możliwości przyjmowania kart. Jednocześnie, z racji wysokiej wartości transakcji, błędne odrzucenie płatności (tzw. False positive) jest w tym przypadku wyjątkowo kosztowne. Warto w tym miejscu nadmienić, że omyłkowe odrzucenie legalnej transakcji niesie ze sobą koszty wykraczające daleko poza samą wartość nominalną odrzuconej transakcji. Klient, którego transakcja została odrzucona, zwykle nie podejmuje kolejnych prób jej realizacji, tylko zwraca się do konkurencji. Co więcej, prawdopodobieństwo, że kiedykolwiek powróci do sprzedawcy, u którego nie udało mu się zapłacić, jest znikome. Innymi słowy, taki błąd jest równoznaczny nie tylko z utratą jednorazowej szansy na sprzedaż, lecz z bezpowrotną utratą klienta.

Jak bezpiecznie płacić kartą za zakupy w Internecie?

Płatności kartą a bezpieczeństwo

W kwietniu 2017 roku, 54% użytkowników Internetu w Polsce zadeklarowało, że dokonało kiedyś zakupów online. Oznacza to, że zakupów w sieci może dokonywać kilkanaście milionów Polaków[8]. Jak płacimy za zakupy? Jest wiele sposobów, począwszy od zrobienia przelewu, przez rozliczenie za pobraniem, do płatności kartą. Te ostatnie to jeden z najszybszych sposobów dokonania płatności (system błyskawicznie rejestruje naszą transakcję, przez co np. wysyłka naszego produktu skraca się o godziny, a czasem nawet i dni), jednak wiele osób wciąż obawia się, że ich dane z karty dostaną się w niepowołane ręce i stracą pieniądze lub nie będą mogły nic zrobić, jeżeli sklep nie prześle towarów lub nie zrealizuje usługi. Oczywiście takie ryzyko występuje, jednak organizacje kartowe oraz banki nas przed nim chronią, umożliwiając najczęściej odzyskanie całej kwoty.

8 gemius.pl/wszystkie-artykuly-aktualnosci/najnowsze-dane-o-polskim-e-commerce-juz-dostepne.html

Chargeback – bezpieczne zakupy w Internecie

Niewielu użytkowników kart płatniczych ma świadomość, jakie prawa przysługują im, gdy ktoś niepowołany użyje danych ich karty do wykonania transakcji lub gdy nie otrzymają zamówionego towaru bądź usługi. Odzyskanie pieniędzy w takich przypadkach umożliwia procedura chargeback. Warunek jest jeden – transakcja musi być przeprowadzona za pośrednictwem karty płatniczej (np. Mastercard, VISA lub Amex). Chargeback pozwala odzyskać pieniądze w przypadku, gdy nie otrzymamy zakupionego przedmiotu (usługi) lub będzie on niezgodny z przedstawioną wcześniej ofertą, w tym także, gdy ktoś inny bez naszej wiedzy i zgody posłużył się naszą kartą do dokonania zakupów w Internecie.

Procedura uzyskania zwrotu środków nie jest skomplikowana. Użytkownik karty, który chce skorzystać z chargebacku, zazwyczaj musi **przedstawić bankowi dowody** potwierdzające zawarcie umowy czy dokonanie płatności – w praktyce jest to wyciąg operacji z karty. W przypadku przyznania racji użytkownikowi karty, bank dokonuje zwrotu kwoty transakcji na rachunek posiadacza karty, a następnie **dochodzi za pośrednictwem organizacji kartowej zwrotu środków od sprzedawcy, który przyjął feralną płatność. Należy zwrócić uwagę, że takiej procedury reklamacyjnej nie można dokonać w przypadku innej metody płatności. Na przykład, jeśli zapłacimy przelewem za towar, którego nie otrzymamy, możemy dochodzić roszczeń jedynie na drodze prawnej, co bywa bardzo czasochłonne, a w przypadku dokonywania zakupów w sklepach zagranicznych zazwyczaj niedostępne dla przeciętnego klienta.**

Maksymalny termin zgłoszenia reklamacji w ramach procedury chargeback zależy od tego, jaki jest powód zgłoszenia. Może to być pomiędzy 45 a 540 dni od dnia wykonania transakcji, czyli czasu jest wystarczająco dużo, żeby zorientować się, że padliśmy ofiarą oszustwa. Przy czym dla większości powodów maksymalny termin wynosi do 120 dni po planowanej dacie dostarczenia usługi. Jeżeli chodzi już o zwrot pieniędzy na naszą kartę, to jest to kwestia indywidualna. Zgodnie z procedurami jednego z wydawców kart płatniczych, agent rozliczeniowy ma 45 dni na udzielenie odpowiedzi bankowi. Po tym czasie powinniśmy spodziewać się pieniędzy na naszym koncie. Jednak konkretną informację na ten temat możemy otrzymać od naszego banku.

Płatność kartą a potencjalne niebezpieczeństwa

Niestety, niezależenie od stosowanych zabezpieczeń, często sami narażamy się na ryzyko utraty środków. Wielu internautów daje się nabrać na podejrzane linki, e-maile czy SMS-y, które otrzymują od anonimowych adresatów i co najgorsze wykonują polecenia zawarte w tych wiadomościach. Jest to jak wpuszczenie złodzieja prosto do naszego mieszkania. Mimo że ryzyka te nie dotyczą bezpośrednio płatności kartą przez Internet, ważne jest, aby bezpiecznie korzystać z komputera, tj. nie wchodzić na podejrzane strony czy ignorować wiadomości od nieznajomych.

Kolejnym rodzajem wyłudzeń jest prośba o podanie haseł do banku czy PIN-u do naszej karty. Podczas dokonywania transakcji kartą online nigdy nie powinniśmy zostać poproszeni o podanie tych

wrażliwych informacji. Do autoryzacji karty kredytowej w wypadku płatności internetowych służy numer CVV, który znajduje się na odwrocie karty – są to trzy cyfry wydrukowane przy pasku do podpisu. Ewentualnie możemy zostać przekierowani na stronę naszego banku, gdzie będziemy musieli wpisać hasła do naszego konta oraz w celu dodatkowej weryfikacji otrzymamy kod SMS-em do potwierdzenia transakcji. Bank nigdy nie wysyła e-maila z prośbą o podanie danych karty w celu weryfikacji płatności.

Na szczęście, każda karta ma określony limit. Nawet jeżeli dojdzie do wyłudzenia za pomocą karty płatniczej, to przestępcy nie będą w stanie przekroczyć pewnej kwoty, którą możemy zazwyczaj sami ustalić dobierając ją do swoich aktualnych potrzeb. Kiedy odkryjemy podejrzaną transakcję wykonaną naszą kartą, należy bezzwłocznie skontaktować się z bankiem, aby zastrzec kartę. Ponadto, w takim wypadku także możemy skorzystać z procedury chargeback w celu odzyskania utraconych pieniędzy.

Do przykładów nadużyć związanych z używaniem karty należą:

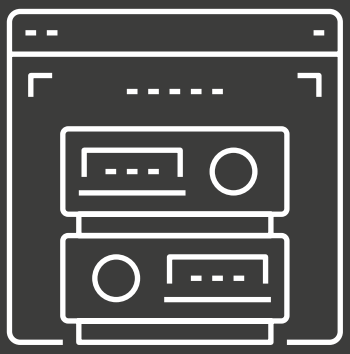
- sytuacja, gdzie posiadacz karty zostaje obciążony za transakcję, w której nie brał udziału bądź której nie autoryzował,
- **nieotrzymanie przez posiadacza dóbr lub usług**, za które została pobrana zapłata,
- phishing - polega na zdobywaniu nieuczciwymi metodami poufnych informacji, dotyczących określonej osoby. Najczęściej oszuści podają się za godną zaufania firmę lub osobę, która potrzebuje w danym momencie określonych danych osobowych/płatniczych,
- oszustwa loteryjne - oszukany dostaje e-mail z wiadomością, że został zwycięzcą loterii i w celu odebrania nagrody powinien skontaktować się z organizatorem konkursu i podać dane karty.

Dlatego też należy pamiętać o kilku prostych zasadach:

- nigdy nie podajemy hasła do konta lub haseł jednorazowych w mailach, wiadomościach, na stronie banku, która nie ma w adresie https://,
- w Internecie nigdy nie używamy PIN-u karty,
- nie umieszczamy zdjęć naszej karty w Internecie, w szczególności na portalach społecznościowych,
- ustalamy limit wartości transakcji na karcie i dostosowujemy go na bieżąco w zależności od naszych aktualnych potrzeb,
- jeżeli coś pójdzie nie tak, informujemy wystawcę karty – mamy dostęp do efektywnych procedur reklamacji.

Karty są bardzo wygodną metodą dokonywania płatności za zakupy w Internecie. Dodatkowo dzięki procedurze chargeback oraz odpowiedniemu zarządzaniu limitami transakcji jest to bardzo bezpieczna forma płatności, która jako jedyna zapewnia ochronę również w przypadku nieotrzymania zamówionego towaru lub usługi. Oczywiście zawsze należy pamiętać, aby nie udostępniać osobom trzecim danych naszej karty oraz w sposób bezpieczny korzystać z komputera.

Omówienie wyników badania



O badaniu

Ze względu na brak szczegółowych danych o zjawisku oszustw płatniczych (fraudu płatniczego) na polskim rynku e-commerce, firmy Nethone oraz EY wspólnie przeprowadziły badanie, którego celem było sprawdzenie skali i percepcji problemu wśród polskich sklepów internetowych. Badanie przeprowadzono metodami CATI i CAWI (w zależności od preferencji respondentów) na grupie 150 przedsiębiorstw. Każde ze zbadanych przedsiębiorstw charakteryzowało się rocznymi obrotami w kanałach online na poziomie co najmniej 100 mln zł. Osobami udzielającymi odpowiedzi na pytania byli członkowie zarządów, dyrektorzy finansowi oraz wskazani przez przedsiębiorstwa decydenci w zakresie zakupów rozwiązań z obszaru bezpieczeństwa IT i zarządzania ryzykiem. Spośród firm-respondentów, 99% prowadzi sprzedaż online na rynku krajowym, 42% sprzedaje swoje produkty/usługi klientom z Unii Europejskiej, 8% klientom z USA, a 7% klientom z Rosji, Ukrainy i innych państw.

Specyfika polskiego rynku e-commerce. Udział poszczególnych metod płatności i wpływ ich struktury na występowanie fraudu płatniczego

Zrozumienie wyników przeprowadzonego badania wymaga w pierwszej kolejności omówienia specyfiki polskiego rynku e-commerce, który zarówno na tle światowych rynków, jak i rynków europejskich cechuje się występowaniem charakterystycznych dla niego zjawisk. Po pierwsze, polski handel online odznacza się dużym rozdrobnieniem przy jednoczesnym występowaniu bardzo nielicznej grupy dużych podmiotów. Po drugie, nie są na nim praktycznie obecni najwięksi światowi gracze, co jest jednocześnie przyczyną i skutkiem bardzo silnej pozycji wąskiego grona lokalnych potentatów. Po trzecie, dzięki nowoczesności i otwartości na innowacje tutejszego sektora bankowego, struktura preferowanych przez konsumentów metod płatności znacząco różni się od struktury dominującej na większości rozwiniętych rynków. Wszystkie te czynniki razem kształtują krajobraz polskiego e-commerce, a co za tym idzie, również specyfikę problemu fraudowego wśród Polskich firm.

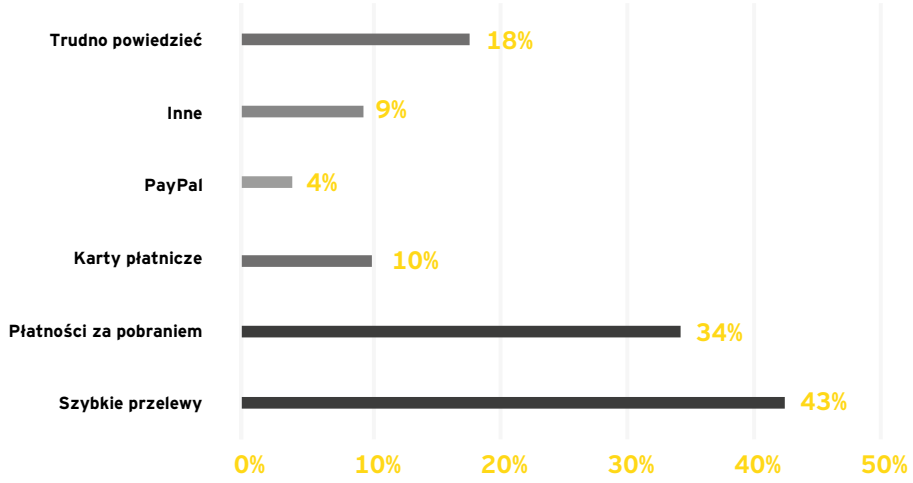
Inaczej niż w USA czy na rynkach tzw. „starej Unii", gdzie handel internetowy zdominowany jest przez duże podmioty działające globalnie i budujące własną infrastrukturę sprzedażową, w Polsce działa wiele małych firm prowadzących sprzedaż za pomocą gotowych platform handlowych. W przypadku najmniejszych podmiotów, które są na rynku najliczniejsze, wiodącą platformą jest Allegro – serwis zapewniający im kompletną infrastrukturę do prowadzenia sprzedaży, włącznie z gotowymi rozwiązaniami płatniczymi. W przypadku nieco większych podmiotów, które stawiają na rozwijanie własnych marek e-commerce, popularnością cieszą się natomiast platformy sprzedażowe takie jak Shopify czy Magento, dostarczające infrastrukturę potrzebną do prowadzenia e-sklepu i pozostawiające swoim klientom stosunkowo dużą dowolność w zakresie doboru dostawców i metod płatności.

Kolejną cechą charakterystyczną polskiego rynku handlu online jest znikoma obecność na nim globalnych gigantów, takich jak Amazon czy eBay. Ten ostatni podejmował dwukrotnie próbę zdobycia polskiego rynku i choć jego udział w nim sukcesywnie rośnie, trudno mówić tu o skali porównywalnej z lokalnym liderem, czyli Allegro. Z kolei Amazon, będący największym na świecie graczem w branży e-commerce, również bardzo powoli powiększa swój udział w tutejszym rynku. Dotychczas, najbardziej znaczącym z perspektywy polskiego konsumenta działaniem Amazon było wprowadzenie pełnej polskiej wersji językowej w niemieckiej odsłonie sklepu. W efekcie, największe w Polsce firmy z obszaru e-commerce to niemal wyłącznie podmioty rodzime, do niedawna budujące swoją pozycję głównie lokalnie – wykorzystując nieobecność globalnych gigantów – lecz w ostatnich latach coraz częściej otwierające się również na rynki zagraniczne. Warto także zwrócić uwagę na coraz liczniejsze grono firm, które po uzyskaniu silnej pozycji w handlu detalicznym offline decydują się na rozwój w sieci.

Trzecim charakterystycznym dla polskiego e-commerce elementem jest specyficzna struktura preferowanych przez konsumentów metod płatności. Jej odmienność wynika przede wszystkim

z innowacyjności tutejszego sektora bankowego, który w związku niewielką do niedawna penetracją rynku przez karty kredytowe wykształcił sprawnie działający system szybkich przelewów bankowych pay-by-link. Umożliwiają one dokonywanie płatności online niemal natychmiastowo, z pominięciem organizacji kartowych, za to z udziałem systemów bankowości internetowej, dzięki czemu cieszą się zaufaniem licznego grona kupujących. Zakupy dokonywane za pomocą tej metody nie są chronione opcją obciążenia zwrotnego. Popularne są w Polsce również płatności za pobraniem, co jest w znacznej mierze pochodną ograniczonego zaufania konsumentów do sprzedawców. Kupujący chcą płacić dopiero wówczas, gdy przesyłka dotrze bezpośrednio do ich drzwi. Karty płatnicze jako metoda płatności online są w Polsce dopiero na trzecim miejscu pod względem popularności, jednak w związku z wchodzeniem na tutejszy rynek coraz większej liczby globalnych podmiotów – niejednokrotnie akceptujących wyłącznie karty, Polacy coraz częściej decydują się na regulowanie należności za pomocą kart oraz wykorzystujących je narzędzi e-walletowych.

Metody płatności



Jakie są orientacyjne udziały procentowe poszczególnych metod płatności w Państwa firmie?

Płatności niekartowe. Szybkie przelewy dominują, płatność za pobraniem wciąż popularna

Według wskazań badanych firm[9], najpopularniejszą metodą płatności są szybkie przelewy pay-by-link, które wg aż 90% respondentów odpowiadają za co najmniej 30% transakcji realizowanych w prowadzonych przez nich sklepach internetowych. Wyniki badania pokazują, że jest także spora grupa firm polegających przede wszystkich na tej metodzie płatności – w przypadku 31% badanych firm transakcje za pośrednictwem szybkich przelewów stanowią co najmniej 50% wszystkich notowanych przez nie płatności. Na drugim miejscu plasuje się płatność za pobraniem, dla której co najmniej 30-procentowy udział wskazało 80% badanych przedsiębiorstw. Tak wysokiego udziału nie osiągają żadne inne metody płatności. W przypadku kart, najwyższy udział tej metody płatności zadeklarowany przez respondenta to 25%.

Wysoki udział płatności za pobraniem jest typowy dla rynków rozwijających się i wskazuje na stosunkowo niski poziom zaufania konsumentów do płatności online oraz do sklepów internetowych w ogóle. Przykładowo, na dużym, lecz charakteryzującym się niskim poziomem ubankowienia społeczeństwa, rynku indyjskim płatność za pobraniem wybiera 83% kupujących.[10] Płatność za pobraniem, choć

9 Na pytanie dotyczące średniego udziału poszczególnych metod płatności w generowaniu całkowitego wolumenu sprzedaży odpowiedzi udzieliło 85% respondentów.

10 http://www.businessinsider.com/cash-on-delivery-remains-the-

jest najmniej wygodną spośród dostępnych metod (wymaga przygotowania przez kupującego gotówki), a w dodatku najdroższą – obarczoną kosztami związanymi z rozliczaniem jej za pośrednictwem firmy kurierskiej lub poczty – jest wybierana przez konsumentów chętnie, głównie ze względu na brak konieczności podawania jakichkolwiek danych płatniczych oraz na minimalizację ryzyka utraty środków w razie niezrealizowania przez sprzedawcę zamówienia. Innymi słowy, klienci chcą płacić za towar dopiero, gdy będą mieli pewność, że ich zamówienie zostało zrealizowane. Ta forma płatności jest równocześnie najmniej korzystną z perspektywy sprzedawcy, bo wiąże się z podwyższonym ryzykiem. Sklep internetowy musi ponieść koszty związane z realizacją zamówienia, z przygotowaniem przesyłki i przekazaniem jej firmie kurierskiej, nie mając żadnej gwarancji, że kupujący zamówienie w ogóle odbierze. W razie odmowy przyjęcia przesyłki przez kupującego lub niedoręczenia jej z innych powodów, sprzedawca musi pokryć koszty związane z próbami podjętymi przez firmę kurierską, opłaty za opcję płatności za pobraniem, a także opłaty z tytułu dostarczenia przesyłki z powrotem do nadawcy, czyli do magazynu sklepu internetowego. Według badań firmy Worldpay, w 2014 roku płatności za pobraniem stanowiły zaledwie 6,6% wszystkich transakcji związanych z zakupami w Internecie, a w 2019 roku mają osiągnąć poziom 6,9% - wynikający przede wszystkim z rozwoju e-commerce w krajach rozwijających się. Dla porównania, w USA – na największym światowym rynku e-commerce – udział pobrań w 2014 roku wynosił zaledwie 4%, a w 2019 r. ma spaść do poziomu 3%.[11]

Odwrotnie niż w przypadku płatności za pobraniem, popularny na całym świecie system PayPal cieszy się wg respondentów stosunkowo niewielkim zainteresowaniem polskich konsumentów, jednak trzeba zauważyć, że ta metoda płatności ma ugruntowaną pozycję w różnego rodzaju niszach rynkowych, w szczególności związanych z obrotem dobrami cyfrowymi. Aż 44% badanych w ogóle nie oferuje możliwości dokonywania płatności za pomocą PayPal, przy czym wspomniana nisza widoczna jest w postaci 2% badanych firm, które wskazały tę metodę jako odpowiadającą za co najmniej 30% notowanych przez nich transakcji.

preferred-method-of-payment-in-india-2016-6?IR=T

[11] http://offers.worldpayglobal.com/rs/850-JOA-856/images/GlobalPaymentsReportNov2015.pdf

Płatności kartowe. Powszechna akceptacja i rosnąca popularność

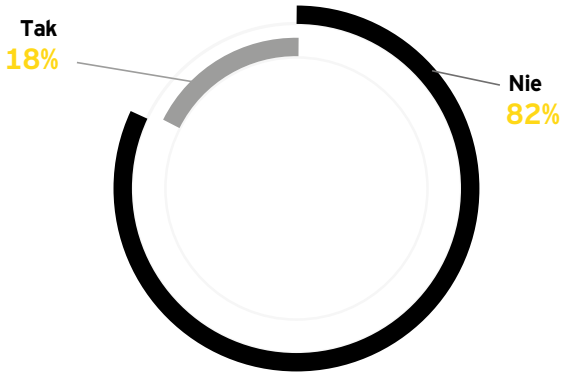
Płatności kartowe, choć na świecie zdecydowanie górują nad wszystkimi innymi metodami, w Polsce cieszą się wciąż stosunkowo niewielką popularnością. Widoczny jest jednak w ich przypadku trend wzrostowy, co w pewnym stopniu wynika z powszechnej akceptacji kart w tutejszych sklepach internetowych. **Aż 95% firm biorących udział w badaniu umożliwia swoim klientom dokonywanie płatności za pomocą karty kredytowej lub debetowej.**

U 65% badanych transakcje dokonywane kartą stanowią od 10 do 30% przyjmowanych płatności, a u 30% mają udział na poziomie poniżej 10%. Jak jednak zwrócono uwagę wcześniej, udział kart sukcesywnie rośnie, co wiąże się z jednej strony z szeroką siecią akceptacji i wpływem globalnych graczy na nawyki płatnicze Polaków, z drugiej – z rozwojem międzynarodowym polskich firm handlujących online. Jeśli spojrzymy na udział kart w wolumenach transakcyjnych podmiotów kierujących ofertę nie tylko do konsumentów z Polski, ale również do klientów z zagranicy (42% badanych), widać, że udział kart rośnie – 78% respondentów handlujących transgranicznie wskazuje udział kart w swoim wolumenie transakcyjnym na poziomie od 10 do 30%. Udział ten będzie prawdopodobnie szybko rósł w nadchodzących latach, dążąc do poziomów prognozowanych dla całego regionu EMEA, gdzie wg przytaczanego już opracowania Worldpay, karty płatnicze (debetowe, kredytowe, obciążeniowe oraz prepaid) będą w 2019 r. odpowiadały za ok. 44% wszystkich transakcji e-commerce (dokładnie tyle samo, ile w prognozach dla całego świata). **Wraz z rosnącym udziałem kart płatniczych, obserwować będziemy z pewnością rosnącą skalę problemu fraudu płatniczego, który podobnie, jak dziś ma to miejsce w globalnym dyskursie, stanie się jednym z kluczowych tematów debaty środowiska związanego z handlem online.**

Percepcja problemu fraudu płatniczego przez polskich sprzedawców internetowych

Pierwszym, co zwraca uwagę w wynikach przeprowadzonego badania, jest niewielka skala problemu fraudu płatniczego wśród polskich sprzedawców online, co zapewne wynika w znacznej mierze z niewielkiego udziału kart płatniczych w ich wolumenach transakcyjnych. Tylko 18% firm zadeklarowało, że miało w ciągu ostatnich 12 miesięcy do czynienia z fraudem, zaś 82% twierdzi, że nie odnotowało w tym okresie ani jednego przypadku wyłudzenia.

Czy w ciągu ostatnich 12 miesięcy Państwa firma miała do czynienia z fraudem płatniczym?

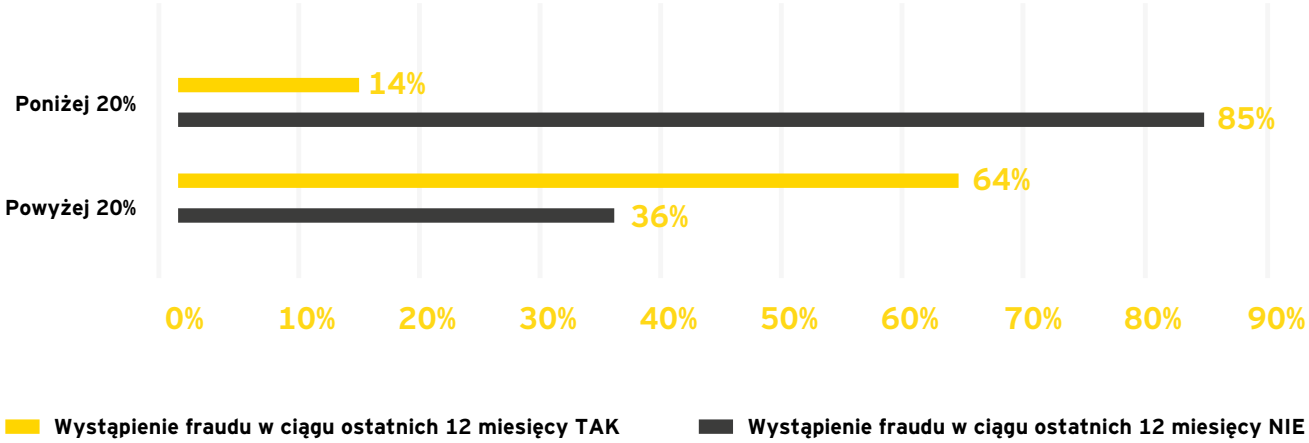


Segmenty szczególnie zagrożone

Z pozoru dane te mogą cieszyć, jednak bliższe spojrzenie na charakterystyki respondentów pozwala potwierdzić tezę, że wraz ze wzrostem udziału kart w wolumenie transakcyjnym, gwałtownie rośnie częstotliwość występowania fraudu. **Spośród firm z udziałem kart jako metody płatności na poziomie powyżej 20%, aż 64% deklaruje, że w ciągu minionych 12 miesięcy odnotowało przypadki fraudu.**

Wyraźnie również widać, podwyższoną częstotliwość występowania fraudu wśród firm handlujących dobrami cyfrowymi, które zresztą często należą również do grupy sprzedawców o znacznym udziale kart w wolumenie transakcyjnym. **56% respondentów z segmentu dóbr cyfrowych deklaruje, że miało w ciągu ostatniego roku do czynienia z fraudami.**

Przybliżony udział kart płatniczych w wolumenie transakcyjnym a przypadki fraudu



W świetle przytoczonych wyników dot. skali zjawiska, nie dziwi, że aż 81% firm deklaruje, iż nie postrzega fraudu płatniczego jako poważnego zagrożenia dla swojego biznesu. W tej części populacji tylko 32% firm sprzedaje poza Polską, podczas gdy wśród firm postrzegających fraud jako problem, aż 85% działa oprócz Polski również na rynkach zagranicznych. Widać również, że w tym gronie karty są relatywnie częściej wykorzystywaną metodą płatności: aż 93% takich respondentów (vs 65% dla całej populacji) ma udział kart na poziomie 10-30%.

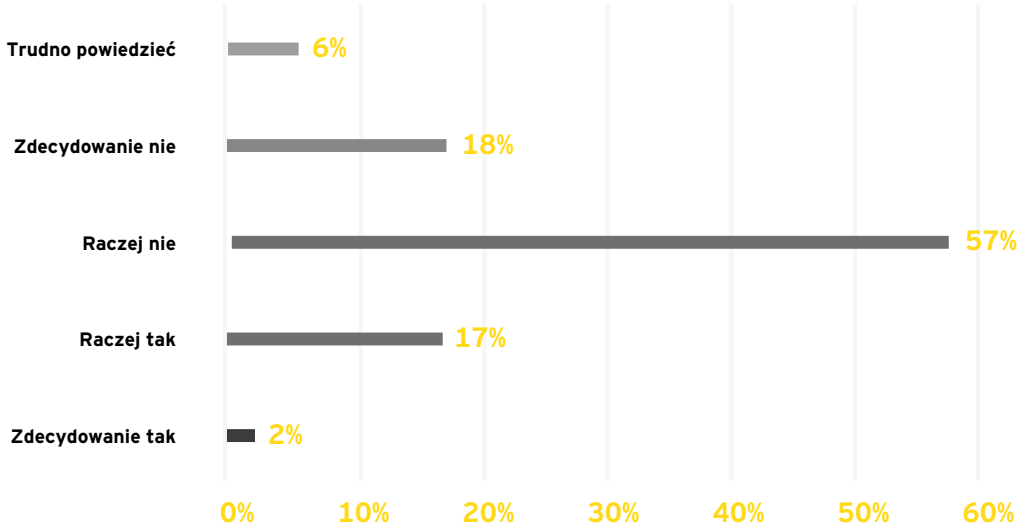
Postrzeganie ryzyka fraudowego pochodną doświadczenia firmy

Analiza wyników wskazuje, że niestety „mądry Polak po szkodzie", gdyż dopiero odnotowanie fraudu zwraca uwagę przedsiębiorstw na istnienie problemu. Postrzeganie fraudu płatniczego jako poważnego zagrożenia wskazało 63% firm, u których takie zdarzenie odnotowano na przestrzeni minionych 12 miesięcy, podczas gdy wśród pozostałych respondentów tylko 9% udzieliło takiej odpowiedzi.

Podobnie sytuacja przedstawia się w odniesieniu do chargebacków, które choć często są konsekwencją odnotowanego fraudu, mogą mieć również inne przyczyny. 37% firm, które odnotowały w ciągu ostatniego roku choćby jeden chargeback, postrzega to jako poważne zagrożenie, zaś spośród pozostałych respondentów takie przekonanie deklaruje zaledwie 5%.

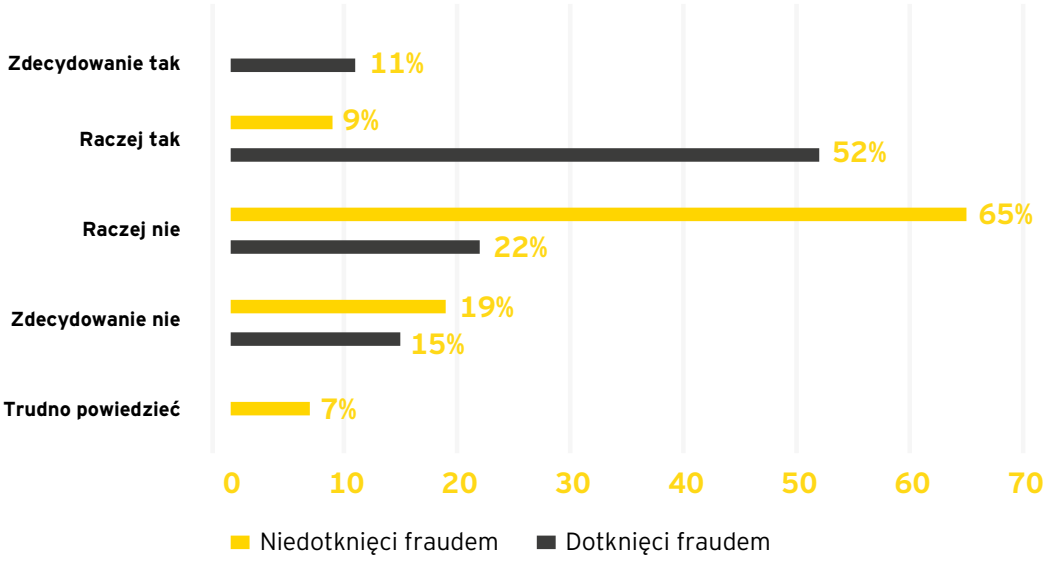
Percepcja fraudu w całej populacji

Czy zjawisko fraudu płatniczego stanowi poważne zagrożenie dla biznesu Państwa firmy?



Percepcja fraudu płatniczego a doświadczenie własne firmy

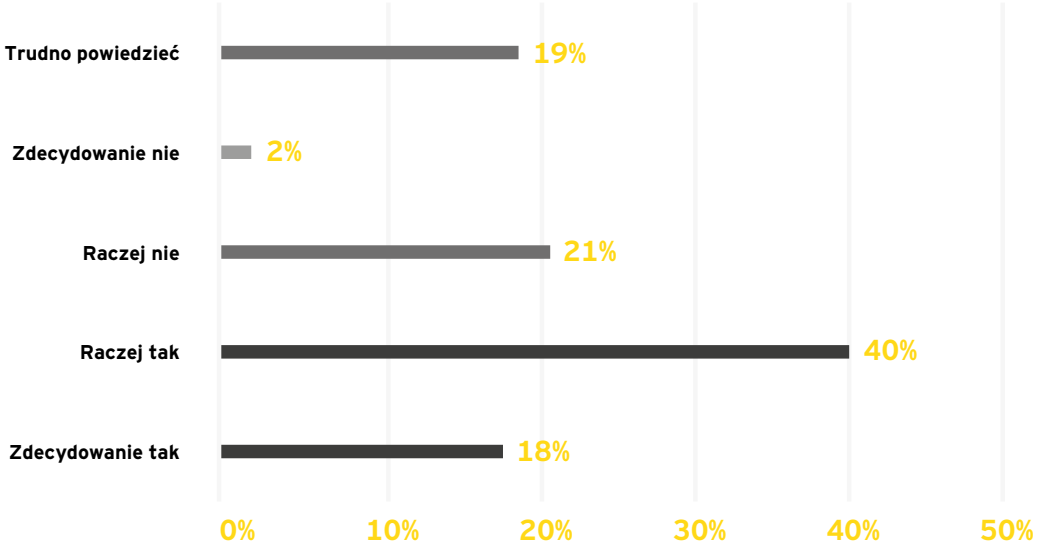
Czy zjawisko fraudu płatniczego stanowi poważne zagrożenie dla biznesu Państwa firmy?



Co ciekawe, badane firmy, zapytane w sposób pośredni o potencjalne straty generowane przez fraud i towarzyszące mu chargebacki, już znacznie częściej deklarowały, że sytuacja, w której takie straty by wystąpiły, byłaby poważnym zagrożeniem dla ich biznesu. Respondenci, pytani o wpływ utraty 0,5% przychodów po około 60 dniach od ich zaksięgowania (czyli opóźnienie typowe dla procedury chargeback), jeśli z fraudem mieli do czynienia, w 67% deklarują, że problem byłby poważny, zaś jeśli z fraudem się nie zetknęli na przestrzeni minionego roku, deklarują to samo w udziale 56%. Innymi słowy, większość firm z polskiego sektora e-commerce postrzega odroczone straty w wysokości 0,5% jako poważne zagrożenie, jednak od tego czy odnotowały w niedalekiej przeszłości u siebie przypadek fraudu zależy, czy wiążą ryzyko utraty środków z tym problemem.

Pole do edukacji i perspektywa zmiany

Czy w przypadku Państwa firmy powtarzająca się konieczność zwrotu 0,5% przychodów po około 60 dniach od ich zaksięgowania byłaby poważnym problemem dla kondycji finansowej firmy?



Polscy sprzedawcy online mają, jak wykazano, stosunkowo niską świadomość występowania i powagi problemu fraudu płatniczego, która w znacznej mierze zależna jest od indywidualnych doświadczeń firm w tym zakresie. Można przewidywać, że wraz z prognozowanym wzrostem udziału kart płatniczych jako wybieranej przez konsumentów metody płatności na polskim rynku będziemy obserwować coraz więcej przypadków fraudu płatniczego, co w konsekwencji będzie miało przełożenie na zwiększanie się świadomości sprzedawców w tym zakresie oraz sposób postrzegania przez nich tego problemu.

O podwyższonej świadomości występowania problemu fraudowego oraz jego percepcji jako poważnego zagrożenia można dziś mówić niemal wyłącznie w przypadku firm, które handlują dobrami cyfrowymi, a także sprzedawców kierujących ofertę do klientów zagranicznych i posiadających wyższy od średniego poziom udziału transakcji kartowych w wolumenie transakcyjnym.

Jak się bronić przed fraudem płatniczym? Jak robią to polskie e-sklepy?

Fraud płatniczy jest tematem tak starym, jak same płatności – występował w różnych formach odkąd tylko człowiek zaczął emitować pieniądz i wystawiać weksle. Można zatem powiedzieć, że fraud płatniczy występuje na świecie tak długo, jak sam handel niewymienny. W nowoczesnym rozumieniu, w odniesieniu do płatności kartowych można o nim mówić od lat '90 XX wieku, a o masowej skali tego typu wyłudzeń, jak zwrócono uwagę w pierwszej części niniejszego opracowania, od jesieni 2015 roku. Nietrudno domyślić się, że w dobie szybkiego rozwoju nowych technologii, na rynku zdążyło ukształtować się wiele rozwiązań mających za zadanie wspierać biznes w zabezpieczaniu się przed wyłudzeniami.

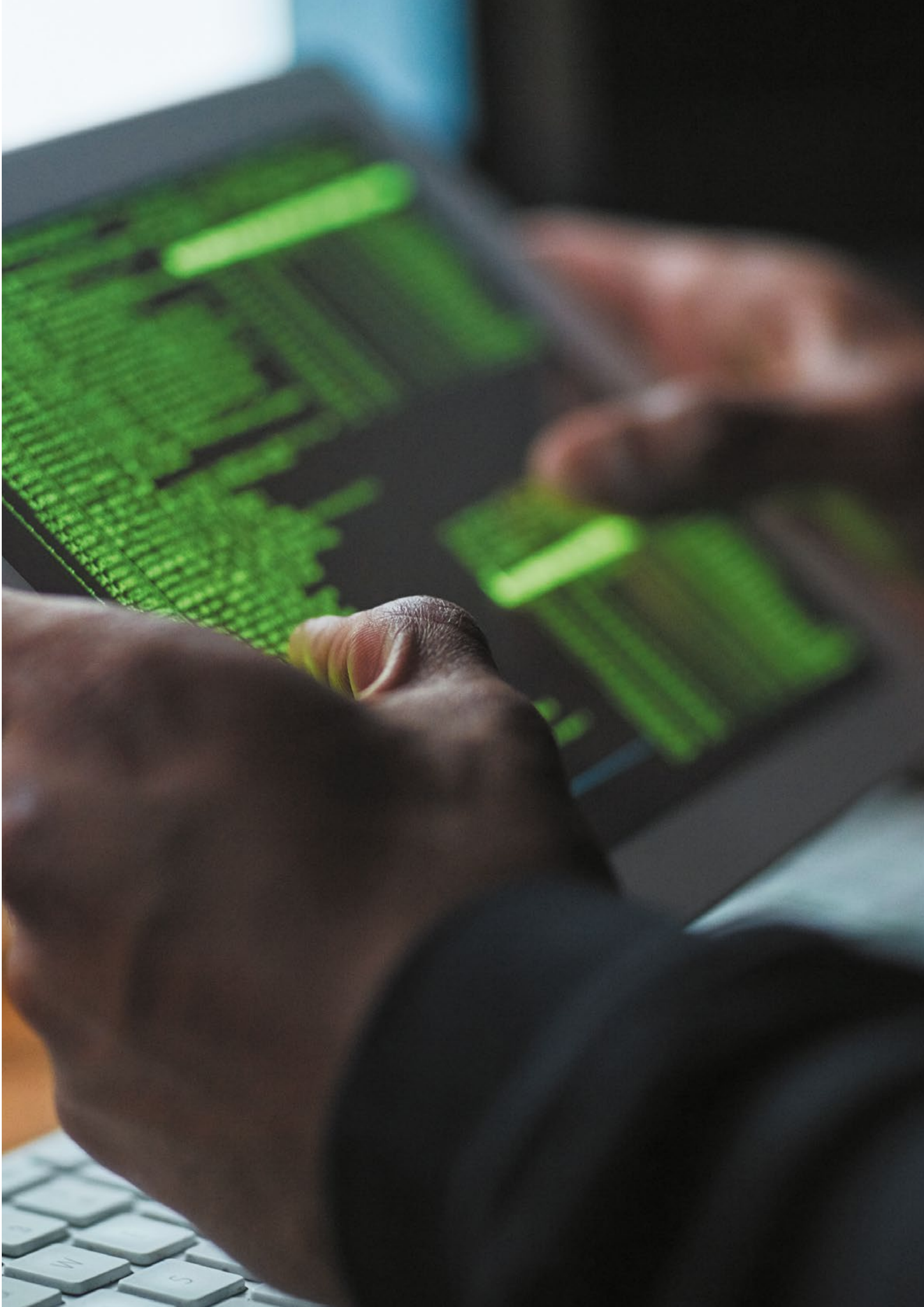
Na niemal wszystkich rynkach, gdzie dominują karty, walka z oszustami należy do obowiązków managerów ryzyka. Są to osoby posiadające specjalistyczną wiedzę w zakresie sposobu działania przestępców internetowych i handlu online, potrafiące na podstawie własnego doświadczenia, badań i obserwacji zdefiniować symptomy fraudu. Co oczywiste, takie osoby nie są w stanie „obejrzeć" każdej pojedynczej transakcji, dlatego też posiłkują się różnego rodzaju rozwiązaniami technicznymi, które mają za zadanie ułatwić im pracę. Dwie najważniejsze kategorie rozwiązań to systemy oparte na regułach oraz systemy wykorzystujące uczenie maszynowe.

Systemy oparte na statycznych regułach

W tradycyjnym wydaniu – dominującym wciąż w świecie e-handlu – managerowie ryzyka korzystają z oprogramowania do filtrowania transakcji w oparciu o zbiory reguł tworzonych przez nich na podstawie eksperckiego know-how. Doświadczony specjalista wie, że transakcje z określonych krajów, dokonywane za pomocą określonych typów kart są obarczone podwyższonym ryzykiem wystąpienia oszustwa. Tworzy więc zestawy reguł, na podstawie których w sposób automatyczny, w razie wystąpienia danych parametrów transakcje są blokowane lub kierowane do manualnej weryfikacji – np. telefonicznej.

Managerowie ryzyka, chcąc dobrze zabezpieczyć biznes przed oszustami w warunkach złożoności świata e-handlu, tworzą coraz więcej reguł, zgodnie z którymi transakcje są przyjmowane, odrzucane lub kierowane do ręcznej weryfikacji. Reguły stają się coraz bardziej skomplikowane i wzajemnie ze sobą powiązane, a co za tym idzie, coraz trudniejsze do szybkiej aktualizacji. Tymczasem, wystarczy niewielka zmiana w sposobie działania oszustów, by zestaw reguł stał się nieskuteczny. Konieczna jest wówczas przebudowa logiki antyfraudowej, co wymaga czasu, wysiłku i pieniędzy.

Wyobraźmy sobie dla przykładu system, w którym działają reguły mówiące, że transakcja wykonywana za pomocą karty kredytowej wydanej w Polsce przez użytkownika znajdującego się w Chicago,



gdy w stanie Illinois jest noc, powinna zostać odrzucona jako potencjalna próba oszustwa. Po pierwsze, w wyniku działania takiego zestawu, Polak mieszkający w USA, lecz posiadający też rachunek w polskim banku nie dokona zakupu, co jest równoznaczne ze stratą. Po drugie, jeśli faktycznie tego typu transakcje okazywały się ostatnio w większości wyłudzeniami, wystarczy, że oszust zamiast z amerykańskiego IP, zacznie korzystać np. z adresu niemieckiego. Pora dnia w Chicago traci w tym momencie znaczenie, a transakcja zostanie przyjęta i poskutkuje chargebackiem. Specjaliści muszą w takiej sytuacji najpierw wykryć zmianę w działaniu oszustów, a następnie zmodyfikować reguły tak, by uwzględniały niemieckie adresy IP jako obarczone podwyższonym ryzykiem.

Managerowie ryzyka poświęcają czas i energię na budowanie zestawów reguł i ich ciągłe kompleksowe aktualizowanie, podczas gdy przestępcy potrafią jedną zmianą zniweczyć ich wysiłki. Co więcej, aby reguły działały z wysoką dokładnością, muszą bazować na dużych zbiorach danych opisujących każdego użytkownika danego sklepu internetowego. Nie sposób przecież odrzucać transakcje tylko dlatego, że pochodzą z jakiegoś konkretnego kraju lub są dokonywane w określonych godzinach. To uniemożliwiłoby skuteczne działanie każdemu biznesowi internetowemu kierującemu ofertę do klientów z różnych krajów. Konieczne jest zatem pozyskiwanie rzetelnych danych i ich dogłębna analiza. Jedno i drugie stanowi poważne wyzwanie. Odpowiedzią na nie są nowego typu systemy – bazujące na sztucznej inteligencji. Co istotne, przedstawione poniżej modele działania, zgodnie z deklaracjami zbadanych firm, niemal w ogóle nie są dziś stosowane w polskim e-commerce, co może mieć dotkliwe konsekwencje, gdy udział kart płatniczych wśród metod płatności wybieranych przez polskich konsumentów zwiększy się, osiągając poziom zbliżony do prognozowanego dla świata i regionu EMEA, do którego Polska przynależy.

Systemy oparte na sztucznej inteligencji

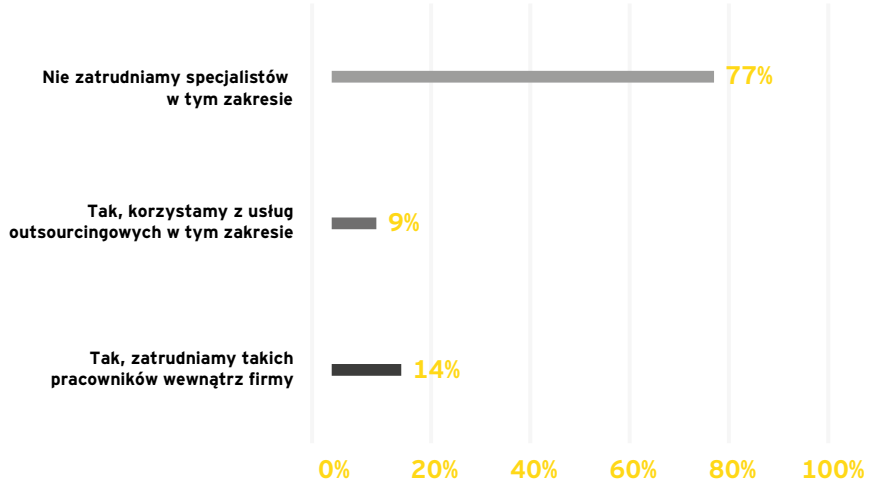
Systemy oparte na sztucznej inteligencji, wykorzystują specjalne algorytmy, przygotowane w taki sposób, by automatycznie analizowały dane dotyczące każdego użytkownika dokonującego transakcji i na podstawie tych danych dokonywały celnych predykcji odnośnie tego czy dana operacja jest próbą wyłudzenia, czy też nie. Oczywiście, odpowiednie przygotowanie modeli i pozyskanie właściwych danych leży po stronie dostawcy systemu antyfraudowego oraz managerów ryzyka. Podstawą stworzenia skutecznego modelu jest nie tylko pozyskanie dużej ilości danych o płacącym i wykorzystywanej przez niego karcie, ale przede wszystkim zrozumienie szerokiego kontekstu, w jakim dochodzi do transakcji. Mowa tu zarówno o kontekście biznesowym – specyfice danej branży – jak również choćby o kontekście kulturowym. Przykładowo, wzmożona transakcyjność w dniach Cyber Monday, Black Friday czy tuż przed Walentynkami, nie powinna nikogo dziwić, choć dla nieodpowiednio przygotowanego systemu mogłaby stanowić sytuację nietypową. Tego typu niuansów jest całe mnóstwo i są one specyficzne nie tylko dla rynku czy branży sprzedawcy, ale również dla określonych grup konsumentów odwiedzających dany sklep internetowy. Odpowiednio „wytrenowane" modele odznaczają się jednak znacznie wyższą skutecznością niż zestawy reguł przygotowywane przez człowieka, ponieważ komputer dysponuje znacznie większymi możliwościami analitycznymi niż człowiek. Co więcej, modele nie wymagają ingerencji człowieka w przypadku zmian w działaniu oszustów. Dzięki ciągłemu uczeniu się i zwiększaniu skuteczności systemu z każdą analizowaną transakcją, modele same adaptują się do zmian. Dzięki temu, managerowie ryzyka mogą skupić się na pogłębianiu swojej wiedzy eksperckiej, analizowaniu rynku i coraz lepszym rozumieniu szerokiego kontekstu, w jakim prowadzona jest sprzedaż, zamiast ręcznie aktualizować rozrośnięte zestawy reguł.

Znajomość i użytkowanie rozwiązań antyfraudowych w polskim e-commerce

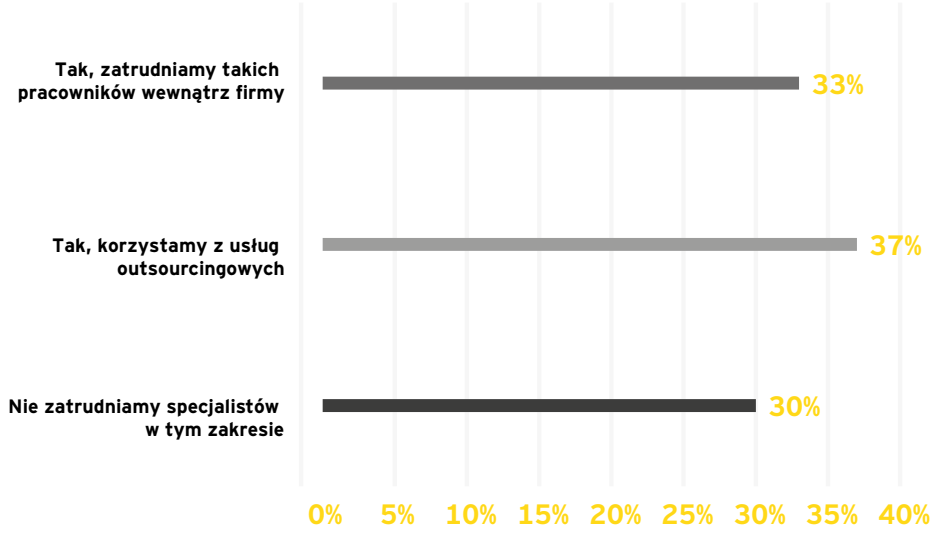
Jak zauważono w rozdziale poświęconym percepcji problemu fraudowego wśród polskich sprzedawców internetowych, stosunkowo niewielka częstotliwość występowania wyłudzeń w polskich sklepach online ma bezpośrednie przełożenie na niski poziom znajomości rozwiązań antyfraudowych w tej grupie.

Zaledwie 23% badanych firm zatrudnia wewnętrznie bądź zewnętrznie managerów ryzyka, przy czym odsetek ten jest znacznie wyższy wśród firm, które zetknęły się w ciągu ostatnich 12 miesięcy z fraudem. W tej grupie wynosi on aż 70%. Dla porównania, wśród firm, które fraudu nie doświadczyły, jest to tylko 13%.

Czy Państwa firma zatrudnia specjalistów odpowiedzialnych za monitorowanie i analizę strumienia transakcji (analityków ryzyka) oraz kierowanie wybranych transakcji na określone ścieżki weryfikacyjne (tzw. manual review)?



Zatrudnianie managerów ryzyka przez firmy dotknięte fraudem



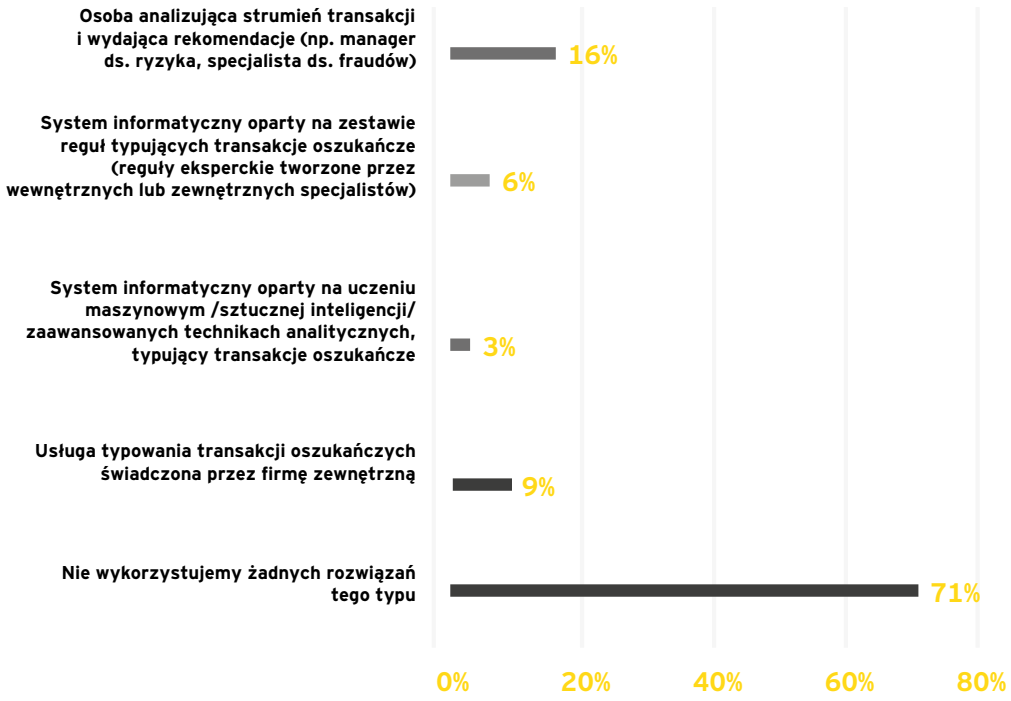
Z powyższych danych można wywnioskować, że historyczne występowanie przypadków fraudu skłania firmy do zatrudniania specjalistów, jednak istnieje też prawdopodobieństwo, że część rynku, w której specjalistów się nie zatrudnia a problem bagatelizuje, zwyczajnie nie monitoruje ryzyka i nie zdaje sobie sprawy z zagrożenia.

Wyniki badania wyraźnie wskazują, że polski e-commerce jest głęboko podzielony, jeśli chodzi zarówno o świadomość problemu fraudowego, jak i umiejętności radzenia sobie z nim. Na rynku dominują firmy o niskiej świadomości problemu, charakteryzujące się brakiem jakichkolwiek rozwiązań analitycznych czy proceduralnych w tym obszarze, nie wspominając już o rozwiązaniach technicznych. Dla kontrastu, wyraźnie widoczna jest stosunkowo mało liczebna grupa podmiotów o wysokiej świadomości, stosujących nowoczesne rozwiązania.

Spośród wszystkich badanych, tylko 35% respondentów ma wdrożone procedury zapobiegania chergebackom, podczas gdy wśród firm, które zetknęły się z przypadkami fraudu, odsetek ten wynosi 74%. Dla porównania, wśród firm, które z fraudem się w ostatnim roku nie zetknęły, jest to tylko 26%.

Aż 71% respondentów nie wykorzystuje żadnego rozwiązania technologicznego służącego do ograniczania fraudów płatniczych. Tutaj również widać dużą zależność pomiędzy doświadczeniem własnym firmy z przypadkami fraudu a stosowaniem odpowiednich systemów zabezpieczających. 67% respondentów, którzy zetknęli się z fraudem płatniczym wykorzystuje rozwiązania ograniczające ryzyko wystąpienia wyłudzeń, podczas gdy w części populacji niedotkniętej fraudem takie rozwiązania stosuje tylko 21% podmiotów. To pokazuje, że „przepaść" między biznesem świadomym i nieświadomym zagrożeń fraudowych jest ogromna.

Czy w Państwa firmie wykorzystywane są któreś z wymienionych niżej rozwiązań, pomagających ograniczyć fraudy?



Jak zabezpieczają się świadomi?

Firmy korzystające z rozwiązań technicznych do minimalizacji ryzyka wystąpienia fraudu stanowią zaledwie 29% badanej populacji. Firmy te stosują równolegle rozwiązania regułowe oraz oparte na uczeniu maszynowym (odpowiednio 20% i 11% w tej grupie). Widać zatem, że rozwiązania nowej generacji dopiero zdobywają popularność wśród firm o wysokim stopniu świadomości w zakresie problemu fraudowego. Co ciekawe, tylko niewiele ponad połowa firm (55%) korzystających z takich systemów zatrudnia managera ryzyka, a stosunkowo liczna grupa firm (45%) bazuje wyłącznie na rozwiązaniach technologicznych.

Analizując dane dot. firm korzystających z rozwiązań technicznych do zapobiegania fraudom, łatwo dostrzec również wyraźną tendencję do przechodzenia od rozwiązań implementowanych w ramach własnej infrastruktury IT sklepu internetowego, do systemów dostarczanych zdalnie, w formie usługi (SaaS – Software as a Service). Podmioty bazujące na własnej infrastrukturze IT stanowią nadal większość (68% respondentów korzystających z rozwiązań technicznych do zapobiegania fraudom), jednak udział firm polegających na rozwiązaniach typu SaaS wynosi już 32% i można spodziewać się, że będzie rósł.

Zwrot z inwestycji, czyli opłacalność systemów antyfraudowych

Firmy, które korzystają z rozwiązań zapobiegających fraudom płatniczym, widzą konkretne zyski z ich stosowania. 64% respondentów z tej grupy wysoko ocenia skuteczność stosowanych w ich firmie rozwiązań, przy czym jednocześnie 75% z nich uważa, że firma mogłaby zwiększyć swoje zyski, podnosząc jeszcze bardziej skuteczność detekcji fraudów.

Wyniki te pokazują, że firmy korzystające z technicznych rozwiązań antyfraudowych, widzą w tym obszarze dużo przestrzeni do poprawy efektywności. Tę przestrzeń starają się zapełnić zaawansowane rozwiązania oparte na sztucznej inteligencji.

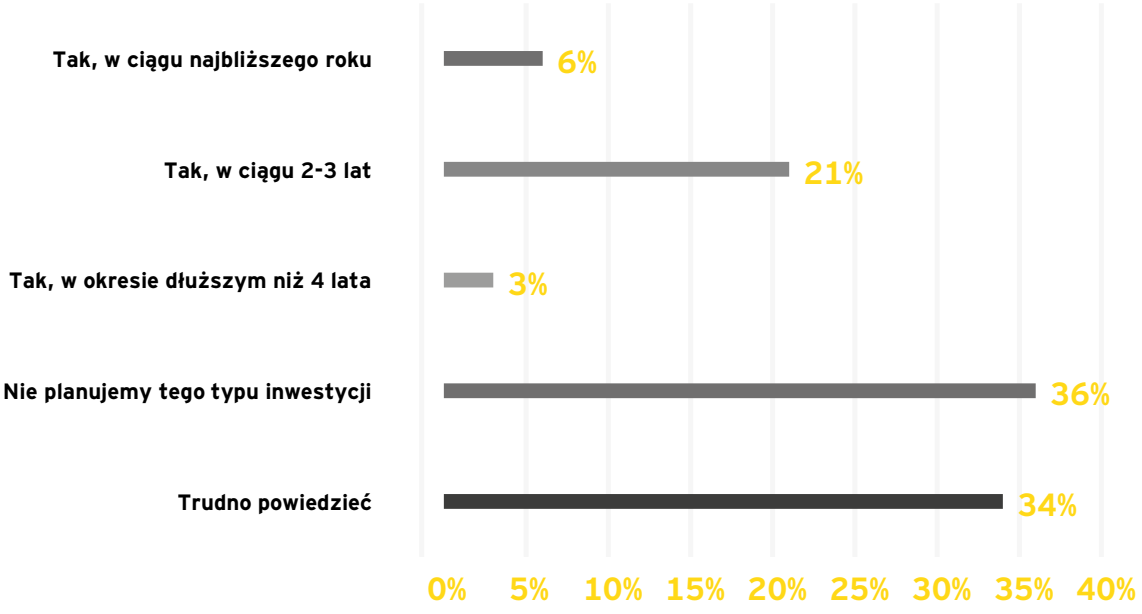
Jak wykazało badanie, inwestycje przedsiębiorstw w nowoczesne systemy antyfraudowe będą w najbliższych latach coraz częstsze – w szczególności wśród przedsiębiorstw, które fraudu już doświadczyły. Istnieje wysokie prawdopodobieństwo, że dołączą do tego grona kolejne przedsiębiorstwa – gdy tylko padną ofiarą fraudu i zrozumieją problem.

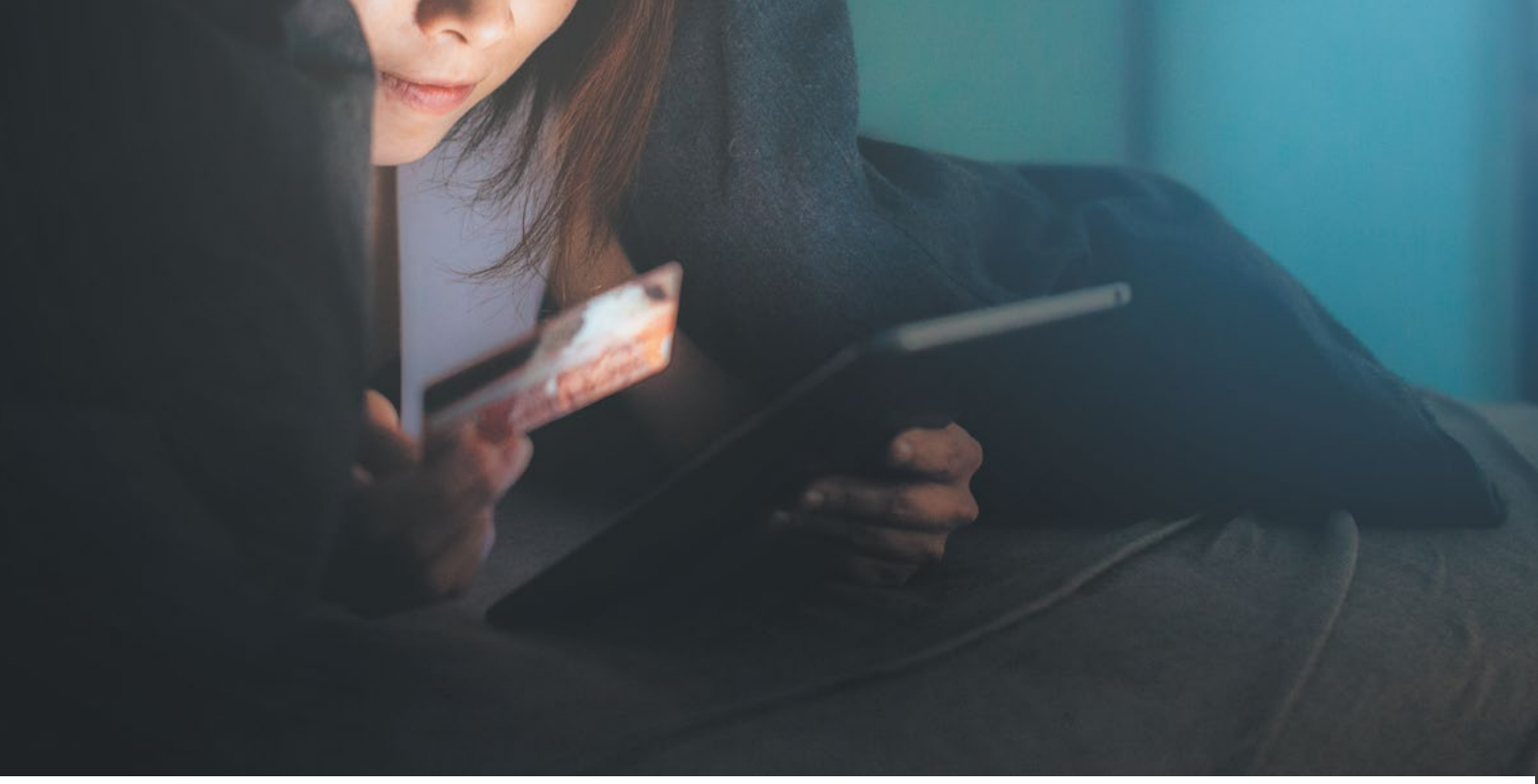
Wyraźnie widać, że plany inwestycyjne w zakresie zapobiegania fraudom płatniczym są zależne bezpośrednio od doświadczenia własnego firm. 81% firm, które doświadczyły fraudu, jest gotowych zainwestować w rozwiązania antyfraudowe, przy czym 56% planuje tego typu inwestycje przeprowadzić w ciągu najbliższych dwóch lat. Dla porównania, wśród firm, które fraudu nie doświadczyły, skłonnych do inwestycji w rozwiązania antyfraudowe jest ledwie 36%, a tylko 21% planuje takie inwestycje w ciągu najbliższych 2 lat. Warto zauważyć, że ich nastawienie może się diametralnie zmienić wraz z pierwszymi odnotowanymi chargebackami i zrozumieniem potencjalnych konsekwencji bagatelizowania problemu.

Planom inwestycyjnym w tym obszarze sprzyja również wysoki (minimum 15%) udział kart płatniczych w wolumenie transakcyjnym sprzedawcy internetowego. 74% firm o takim udziale kart jest gotowych zainwestować w rozwiązania antyfraudowe pozwalające zredukować chargebacki, zaś 71% w ogóle planuje inwestycje w obszarze zapobiegania fraudom w ciągu najbliższych dwóch lat.

Charakterystyczną cechą tej grupy firm jest również przewidywanie, że ich wydatki na zapobieganie fraudom będą rosły. Twierdzi tak aż 54% respondentów z tej kategorii. Powinno to być istotną wskazówką dla pozostałych firm. Sprzedawcy akceptujący stosunkowo dużo kart rozumieją problem fraudu oraz potrzebę skutecznego zabezpieczania się przed nim. Rozumieją też, że problem będzie miał coraz większą skalę, a ich wydatki na zabezpieczenie się przed nim powinny proporcjonalnie rosnąć. Warto jednak podkreślić, że wydatki są w istocie inwestycją, bo w dłuższej perspektywie pozwolą takim biznesom zarobić więcej i uniknąć ryzyka wypadnięcia z rynku. Firmy, które fraudu dotąd nie doświadczyły, wraz z prognozowanym wzrostem popularności płatności kartowych online, mogą łatwo trafić do grona biznesów zagrożonych fraudem całkowicie bezbronne i nieprzygotowane.

Czy Państwa firma planuje inwestycje w obszarze zapobiegania fraudom?





Zagrożeni nieświadomi i utracone korzyści

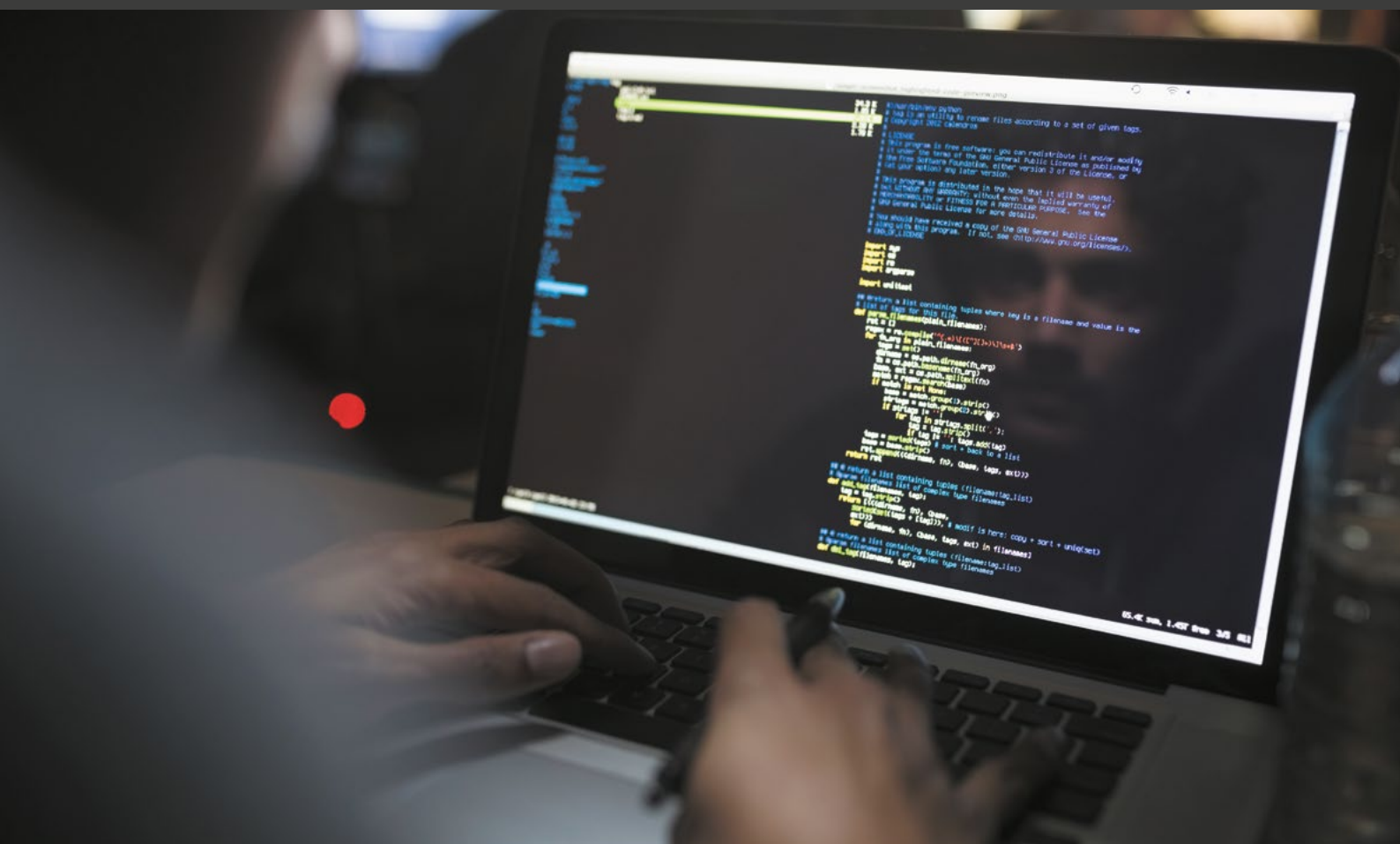
Wśród firm niekorzystających z rozwiązań antyfraudowych nie widać planów zmiany, co może wynikać z opisanej wcześniej stosunkowo niewielkiej w tej części populacji świadomości problemu i jego wagi. Aż 91% takich firm nie planuje wdrażania technicznych rozwiązań antyfraudowych, a 78% nie planuje jakichkolwiek zmian w obszarze przeciwdziałania fraudom płatniczym.

Oznacza to, że przytłaczająca większość dużych polskich sklepów internetowych nie tylko jest bezbronna w starciu z oszustami, ale również nie bierze pod uwagę zabezpieczania się w świetle prognozowanego wzrostu poziomu ryzyka związanego z nadużyciami w niedalekiej przyszłości – pomimo że już dziś oferuje klientom możliwość płacenia kartą za zakupy.

Badanie wykazało również, że firmy, które z problemem fraudu się dotąd nie zetknęły - przez co nie miały okazji robić przeglądu rynku rozwiązań zabezpieczających - nie wiedzą, że wysokiej klasy systemy antyfraudowe oferują znacznie więcej możliwości niż tylko przewidywanie prób wyłudzeń. W konsekwencji większość dużych polskich e-sprzedawców nie wykorzystuje szansy na zwiększenie sprzedaży, jaką niosą dobre systemy antyfraudowe. Dane pozyskiwane do analiz związanych z oceną ryzyka mogą być z powodzeniem wykorzystywane do celnego wnioskowania w różnych aspektach biznesu. Świadomość korzyści, jakie przynoszą rozwiązania dostarczające szczegółowych informacji na temat użytkowników strony/aplikacji, posiada zdecydowana większość ankietowanych firm (81% wszystkich badanych). Równocześnie, co nie zaskakuje, ta świadomość jest największa wśród biznesów korzystających z rozwiązań antyfraudowych (92%) oraz mających wysoki – co najmniej 15-procentowy – udział kart w wolumenie transakcyjnym (91%). Firmy, które nie planują inwestycji w systemy antyfraudowe, najwyraźniej nie łączą walki z wyłudzeniami z możliwością zwiększania sprzedaży.

Sztuczna inteligencja i profilowanie w walce z wyłudzeniami

Obecnie na rynku są dostępne rozwiązania, które wykorzystują głębokie, wielowymiarowe profilowanie użytkowników, a także zaawansowane uczenie maszynowe. Narzędzie profilujące jest w stanie dogłębnie „prześwietlić" każdego użytkownika sklepu internetowego lub aplikacji natywnej, zbierając przy tym tysiące punktów danych charakteryzujących jego sprzęt, oprogramowanie, środowisko sieciowe oraz zachowanie w interakcji z serwisem (biometria behawioralna). Dane te są dodatkowo wzbogacane o informacje istotne kontekstowo – dobierane indywidualnie do potrzeb i specyfiki sprzedawcy internetowego. Zarówno analizy służące odpowiedniemu skonfigurowaniu modeli antyfraudowych, jak i sama ochrona przed wyłudzeniami realizowane są za pomocą specjalnych modeli uczenia maszynowego. Modele tworzone są indywidualnie dla każdego klienta ze względu na mnogość unikalnych dla każdej firmy uwarunkowań. Celem systemów opartych na uczeniu maszynowym jest detekcja oszustów jeszcze zanim podejmą próbę wyłudzenia. Ponieważ profilowanie użytkowników wymaga przetwarzania dużych ilości danych, stwarza ono możliwości wykraczające poza zwalczanie fraudów. Dane można wykorzystać do przygotowywania i trenowania modeli dokonujących innego rodzaju predykcji. Przykładowo, system może służyć do prowadzenia automatycznej, adaptacyjnej segmentacji użytkowników, do przewidywania istotnych wskaźników, takich jak LTV, MRR czy stopa odpływu użytkowników. Predykcje i rekomendacje, podobnie jak w przypadku zwalczania wyłudzeń, są wówczas wydawane w czasie rzeczywistym, dzięki czemu sklep internetowy może indywidualnie, na bieżąco kształtować doświadczenie zakupowe dla każdego klienta, podejmować odpowiednie działania prewencyjne w razie zagrożenia jego rezygnacją z zakupów czy też z wysoką precyzją przewidywać jego przyszłe decyzje zakupowe.



Podsumowanie

Wnioski

1 Specyficzna struktura polskiego rynku pod względem preferowanych przez konsumentów metod płatności (dominacja pay-by-linków – 43% i płatności za pobraniem – 34%) implikuje **stosunkowo niski poziom świadomości tutejszych e-sprzedawców w zakresie zagrożenia fraudem płatniczym**.

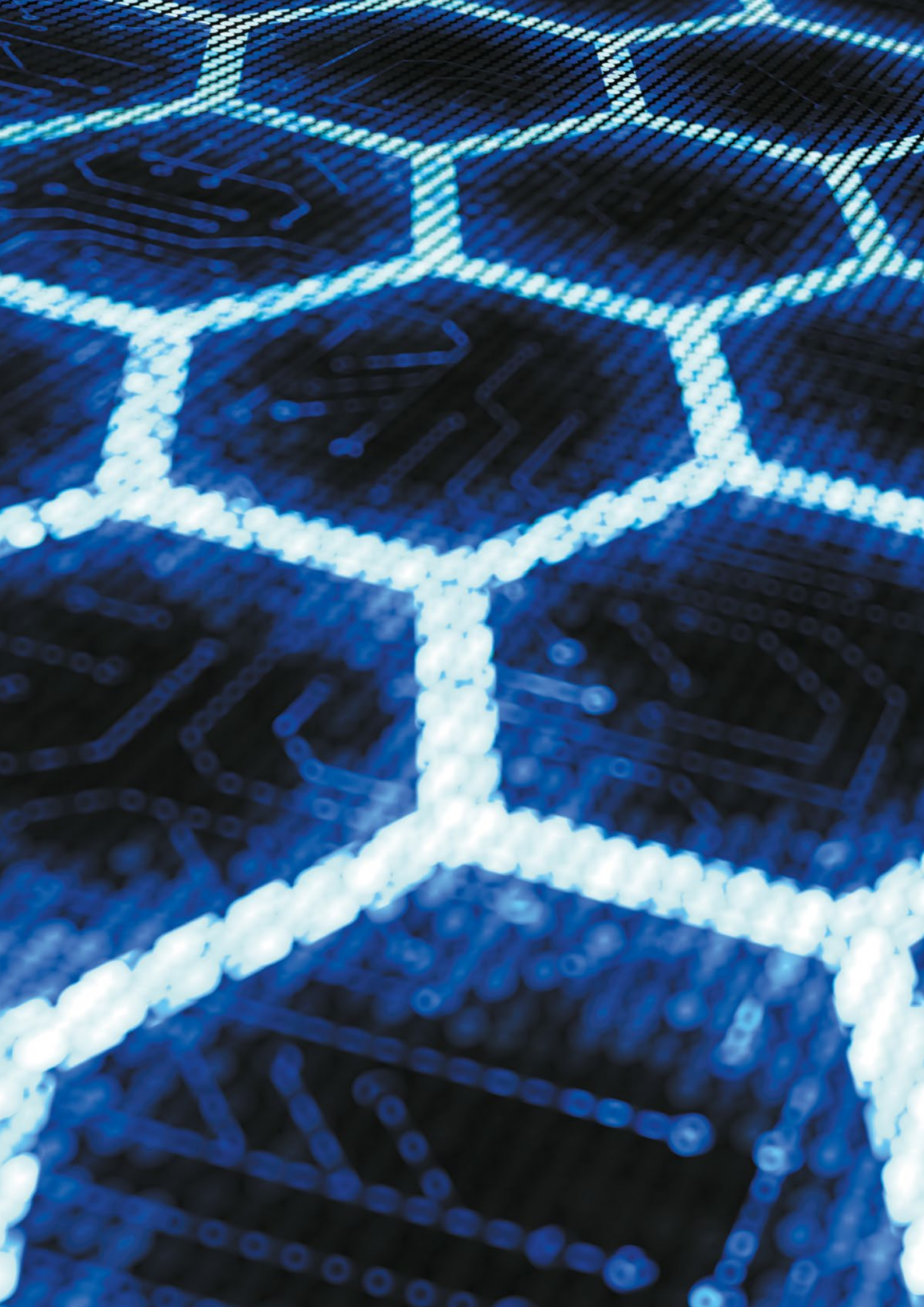
2 **Podwyższonym poziomem świadomości problemu cechują się firmy, które adresują ofertę do klientów zagranicznych**. W tym gronie widać wyższy niż w całej populacji udział kart płatniczych w generowaniu wolumenu transakcyjnego (najczęstsza odpowiedź to ok. 20% podczas gdy dla firm ograniczających się do rynku polskiego – ok. 15%).

3 Choć polski rynek e-commerce stale rośnie, tempo wzrostu oraz struktura tego rynku (kilku dużych graczy i szerokie grono mikrosprzedawców) wskazują, że **dla polskiego e-commerce szansą na przyspieszony rozwój jest wychodzenie z ofertą poza granice kraju.**

4 **Kierowanie oferty do klientów spoza Polski wiąże się z koniecznością akceptacji kart płatniczych jako kluczowej metody płatności.** Karty są najczęściej wybieraną przez konsumentów metodą w wymiarze globalnym, jak również w skali regionu EMEA.

5 Sprawna, bezpieczna akceptacja kart jest możliwa wyłącznie z zastosowaniem rozwiązań zabezpieczających sprzedawcę przed wyłudzeniami, stanowiącymi obecnie jedno z najpoważniejszych wyzwań dla światowego e-handlu. W przypadku tzw. branż podwyższonego ryzyka – szczególnie zagrożonych fraudem płatniczym – celna detekcja nadużyć jest warunkiem koniecznym dla funkcjonowania biznesu na rynku. **Do branż wyjątkowo zagrożonych zaliczyć można m.in. dobra i usługi cyfrowe, gry komputerowe, usługi turystyczne czy dobra luksusowe**.

6 Sklepy planujące ekspansję zagraniczną powinny wdrożyć wysokiej klasy rozwiązania antyfraudowe, uwzględniając przy ich wyborze dostępność opcji wykraczających poza detekcję nadużyć. Większość polskich e-sprzedawców dostrzega ogromną wartość płynącą z wykorzystywania rozwiązań umożliwiających uzyskiwanie szczegółowej, pogłębionej wiedzy o użytkownikach (81% badanych). Kluczem jest więc zrozumienie przez te sklepy, że **dobre rozwiązanie antyfraudowe jest w istocie równocześnie rozwiązaniem stymulującym rozwój**.



EY | Assurance | Tax | Transactions | Advisory

O firmie EY

EY jest światowym liderem rynku usług profesjonalnych obejmujących usługi audytorskie, doradztwo podatkowe, doradztwo biznesowe i doradztwo transakcyjne. Nasza wiedza oraz świadczone przez nas najwyższej jakości usługi przyczyniają się do budowy zaufania na rynkach kapitałowych i w gospodarkach całego świata. W szeregach EY rozwijają się utalentowani liderzy zarządzający zgranymi zespołami, których celem jest spełnianie obietnic składanych przez markę EY. W ten sposób przyczyniamy się do budowy sprawniej funkcjonującego świata. Robimy to dla naszych klientów, społeczności, w których żyjemy i dla nas samych.

Nazwa EY odnosi się do firm członkowskich Ernst & Young Global Limited, z których każda stanowi osobny podmiot prawny. Ernst & Young Global Limited, brytyjska spółka z odpowiedzialnością ograniczoną do wysokości gwarancji (company limited by guarantee) nie świadczy usług na rzecz klientów. Aby uzyskać więcej informacji, wejdź na www.ey.com/pl

EY, Rondo ONZ 1, 00-124 Warszawa

ey.com/pl

O firmie Nethone

Nethone jest globalnym dostawcą opartych na sztucznej inteligencji rozwiązań KYU (Know Your Users), które pomagają przedsiębiorstwom przekształcać zagrożenia i wyzwania w trafne, dochodowe decyzje biznesowe. Od najwyższej klasy zabezpieczeń przed fraudem, przez działające w czasie rzeczywistym narzędzia do adaptacyjnej segmentacji i retencji klientów, aż po wykorzystujące biometrię behawioralną systemy do zapobiegania przejęciom kont bankowych, rozwiązania Nethone pozwalają firmom równocześnie chronić się przed stratami i zwiększać zyski. Spółkę założyli w 2016 roku doświadczeni specjaliści w dziedzinie data science, eksperci bezpieczeństwa IT oraz wysokiej klasy managerowie związani z branżą finansową. Jest ona obecnie jednym z najszybciej rozwijających się przedsiębiorstw z segmentu FDP w Europie środkowo-wschodniej.

Nethone, Plac Europejski 1, 00-844 Warszawa

nethone.com