Подані до Національного банку України
зауваження і пропозиції до проєкту постанови “Зміни до Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку” від заінтересованих осіб.

№ з/п	Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім’я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
1.	7-1 Надавач платіжних послуг має право не застосовувати посилену автентифікацію користувачів платіжної послуги в таких випадках: 1) виконання транскордонної платіжної операції з використанням реквізитів платіжної картки; 2) виконання платіжної операції в системі S.W.I.F.T.;	Викласти п. 2) в наступній редакції: «2) виконання платіжної операції в системі S.W.I.F.T. та/або ініціювання платіжної операції в системі S.W.I.F.T.;»	Відповідно до пункту 3 статті 68 Закону України «Про платіжні послуги» (надалі - Закон) надавачі платіжних послуг зобов'язані застосовувати посилену автентифікацію користувача під час: 2) ініціювання дистанційної платіжної операції; SWIFT - це міжнародна міжбанківська система	Юридична особа: Акціонерне товариство "Сітібанк"	ЄДРПОУ: 21685485, (bohdan.dmukhovskyy@citi.com)	26.09.2025 17:23:12

	3) здійснення платіжної операції з використанням платіжної картки (в тому числі токенів платіжних карток), що ініціюються за допомогою фізичного платіжного пристрою із застосуванням контактної та безконтактної технології.		передавання інформації та здійснення платежів. SWIFT є засобом дистанційної комунікації, а будь-яка юридична особа, з рахунку якої в банку України ініціюється платіжна операція є користувачем в розумінні Закону України «Про платіжні послуги». При цьому користувач може ініціювати платіжну операцію (передавати надавачу платіжних послуг інформацію з реквізитами необхідними для здійснення платежу) через систему SWIFT; у свою чергу, надавач платіжних послуг на підставі таких інструкцій може виконувати платіжну операцію в інших системах, ніж SWIFT, наприклад: отримання інформації з реквізитами			

			необхідними для здійснення платежу через систему SWIFT від клієнта-нерезидента з подальшим списанням коштів (виконання платіжної операції) із рахунку клієнта-нерезидента в гривнях через СЕП.			
2.	відсутня	Доповнити пунктом 7-2 наступного змісту: "7-2 Надавач платіжних послуг може не застосовувати посилену автентифікацію клієнтів - юридичних осіб при ініціюванні ними електронних платіжних операцій за допомогою спеціалізованих корпоративних платіжних процесів або протоколів, що не пропонуються споживачам. Таке незастосування можливе за умови, що надавач платіжних послуг надасть лист-підтвердження	Включення даного пункту має на меті гармонізацію національного законодавства у сфері платіжних послуг з нормами Європейського Союзу. Це безпосередньо стосується положень Директиви про платіжні послуги (PSD2, Директива (ЄС) 2015/2366) та, зокрема, Статті 17 «Безпечні процеси та протоколи корпоративних платежів» Регламенту Комісії № 2018/389/ЄС від 27 листопада 2017 р., що доповнює Директиву	Юридична особа: Акціонерне товариство "Сітібанк"	ЄДРПОУ: 21685485, (bohdan.dmukhovskyy@citi.com)	26.09.2025 17:28:16

		Національному банку, що ці процеси або протоколи гарантують рівні безпеки, щонайменше еквівалентні вимогам, встановленим законодавством про платіжні послуги."	2015/2366/ЄС Європейського Парламенту та Ради щодо нормативних технічних стандартів для надійної автентифікації клієнтів. Стаття 17 Регламенту (ЄС) 2018/389/ЄС визнає, що корпоративні платники, які не є споживачами, часто використовують внутрішні системи та протоколи, що вже інтегрують високі рівні безпеки. Таким чином, імплементація цього пункту в українське законодавство дозволить забезпечити відповідність українських регуляторних практик європейським стандартам і буде врахувати очікування міжнародних клієнтів, які ведуть активну діяльність та користуються банківськими			

			послугами в ЄС, пропонуючи їм схожий, ефективний та безпечний сервіс в Україні.			
3.	14. Надавач платіжних послуг за результатами процедури посиленої автентифікації користувача платіжної послуги створює код автентифікації. Для створення коду автентифікації надавач платіжних послуг використовує багатоцільові пристрої або програмне забезпечення, призначене для цілей автентифікації користувача платіжних послуг. Код автентифікації повинен бути стійким до його підробки та стійким до розкриття будь-якого з елементів посиленої автентифікації, з	14. Надавач платіжних послуг за результатами процедури посиленої автентифікації користувача платіжної послуги створює **або покладається на інших юридичних осіб, з якими встановлені договірні відносини, щодо створення коду автентифікації.** Для створення коду автентифікації надавач платіжних послуг використовує багатоцільові пристрої або програмне забезпечення, призначене для цілей автентифікації користувача платіжних послуг. Код автентифікації повинен бути стійким до його	Викласти пункт 14 Глави 4 Постанови № 58 у відповідності до статті 4 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017. Article 4 1. Where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code. Або врахувати пропозиції наведені Visa, які адаптовані відповідно для надання	Юридична особа: ПРЕДСТАВНИЦТВО ВІЗА ІНТЕРНЕШНЛ СЕРВІС ЕСОУСІЕЙШН	ЄДРПОУ: 26255401, (Oshvydko@visa.com)	23.09.2025 13:36:30

	використанням яких цей код було створено. Для забезпечення стійкості коду автентифікації надавач платіжних послуг застосовує такі технологічні рішення, як створення та перевірка справжності одноразових паролів, **<u>кваліфікованих електронних підписів, удосконалених електронних підписів з кваліфікованим сертифікатом</u>** чи інші підтвердження з використанням криптографічних засобів захисту інформації, що містяться в елементах посиленої автентифікації.	підробки та стійким до розкриття будь-якого з елементів посиленої автентифікації, з використанням яких цей код було створено. Для забезпечення стійкості коду автентифікації надавач платіжних послуг застосовує такі технологічні рішення, як створення та перевірка справжності одноразових паролів, кваліфікованих електронних підписів, удосконалених електронних підписів з кваліфікованим сертифікатом чи інші підтвердження з використанням криптографічних засобів захисту інформації, що містяться в елементах посиленої	можливості проведення дистанційних платіжних операцій з використанням технологій Click to Pay, Apple Pay, Google Pay та інших.			

		автентифікації.				
4.	45. Надавач платіжних послуг з обслуговування рахунків має право залучити для проведення посиленої автентифікації користувача платіжної послуги іншого надавача платіжних послуг або технологічного оператора платіжних послуг або оператора платіжної системи.	45. Надавач платіжних послуг з обслуговування рахунків має право залучити для проведення посиленої автентифікації користувача платіжної послуги іншого надавача платіжних послуг або технологічного оператора платіжних послуг або оператора платіжної системи **або інших юридичних осіб, з якими встановлені договірні відносини.**	Пропозиції наведені Visa адаптовані відповідно для надання можливості проведення дистанційних платіжних операцій з використанням технологій Click to Pay, Apple Pay, Google Pay та інших.	Юридична особа: ПРЕДСТАВНИЦТВО ВІЗА ІНТЕРНЕШНЛ СЕРВІС ЕСОУСІЕЙШН	ЄДРПОУ: 26255401, (Oshvydko@visa.com)	23.09.2025 13:36:30
5.	10. Надавач платіжних послуг відповідно до вимог пункту 2 глави 1 розділу I цього Положення забезпечує документування заходів безпеки із захисту платіжних операцій, оцінює та перевіряє ці заходи на відповідність вимогам Національного банку щодо захисту	10. Надавач платіжних послуг відповідно до вимог пункту 2 глави 1 розділу I цього Положення забезпечує документування заходів безпеки із захисту платіжних операцій, оцінює та перевіряє ці заходи на відповідність вимогам Національного банку	В українському законодавстві є термін "документ державного зразка" і технічний опис такого документу. Ці документи видаються особам, які закінчили навчальний заклад за акредитованою програмою, акредитація яких	Фізична особа: Дубихвіст Олександр Анатолійович	dubykhvist@gmail.com	23.09.2025 15:42:14

	інформації, кіберзахисту та інформаційної безпеки під час надання платіжних послуг. Перевірки здійснюються відповідальними особами надавача платіжних послуг. Ці відповідальні особи не повинні брати участі в основній операційній діяльності надавача платіжних послуг або надавач платіжних послуг повинен залучати до таких перевірок інших осіб, які є незалежними від надавача платіжних послуг, на підставі відповідних договорів, укладених для цілей перевірки. Такі відповідальні особи повинні мати **сертифікати/дипломи міжнародного та/або державного зразка про здобуття навиків/знань** у сферах захисту інформації та кіберзахисту, безпеки	щодо захисту інформації, кіберзахисту та інформаційної безпеки під час надання платіжних послуг. Перевірки здійснюються відповідальними особами надавача платіжних послуг. Ці відповідальні особи не повинні брати участі в основній операційній діяльності надавача платіжних послуг або надавач платіжних послуг повинен залучати до таких перевірок інших осіб, які є незалежними від надавача платіжних послуг, на підставі відповідних договорів, укладених для цілей перевірки. Такі відповідальні особи повинні мати сертифікати/дипломи ~~міжнародного та/або державного зразка~~ про здобуття навиків/знань	здійснюється державними органами України. Для фахівця з вищою освітою - це діплом про набуття кваліфікації за певною спеціальністю. Отже, треба враховувати, що Постанова КМУ від 29 квітня 2015 р. № 266 "Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти" містить лише обмежений перлік спеціальностей, які відповідають визаначенню п.10 прєкту Постанови щодо "захисту інформації та кіберзахисту, інформаційних технологій". Спеціальність, яка відповідає визначенню "безпеки переказу коштів" взагалі відсутня. Як відсутня			

	переказу коштів та інформаційних технологій.	у сферах захисту інформації та кіберзахисту, безпеки переказу коштів та інформаційних технологій. **Ці дипломи/сертифікати повинні бути або державного зразка, або видані міжнародними організаціями, які здійснюють сертифікацію відповідних фахівців.**	вона і в Міжнародній стандартній класифікації освіти ISCED-F 2013. Термін "диплом міжнародного зразка" взагалі відсутній у термінології українського законодавства і є, скоріш, маркетинговим терміном, ніж юридичним. При цьому є кваліфікаційні сертифікати, наприклад https://www.pcisecuritystandards.org/program_training_and_qualification/ , які не є "сертифікатами міжнародного зразка", але визнаються міжнародними платіжними системами.			
6.	11. Надавач платіжних послуг, який скористався правом не застосовувати посиленої автентифікації користувача платіжних послуг, виконавши вимоги, визначені в главі 12 розділу III цього	11. Надавач платіжних послуг, який скористався правом не застосовувати посиленої автентифікації користувача платіжних послуг, виконавши	В українському законодавстві є термін "документ державного зразка" і технічний опис такого документу. Ці документи видаються особам, які закінчили навчальний	Фізична особа: Дубихвіст Олександр Анатолійович	dubykhvist@gmail.com	23.09.2025 15:42:14

	Положення, здійснює не рідше одного разу на рік обов’язкову перевірку впроваджених заходів безпеки із захисту платіжних операцій, реєстрації випадків шахрайства та розрахованого загального коефіцієнта шахрайства для кожного виду платіжної операції. Відповідальні особи, які здійснюють цю перевірку, не повинні брати участі в основній операційній діяльності надавача платіжних послуг або надавач платіжних послуг 6 залучає до таких перевірок інших осіб, які є незалежними від надавача платіжних послуг, на підставі відповідних правових угод, укладених для цілей перевірки. Такі відповідальні особи повинні мати	вимоги, визначені в главі 12 розділу ІІІ цього Положення, здійснює не рідше одного разу на рік обов’язкову перевірку впроваджених заходів безпеки із захисту платіжних операцій, реєстрації випадків шахрайства та розрахованого загального коефіцієнта шахрайства для кожного виду платіжної операції. Відповідальні особи, які здійснюють цю перевірку, не повинні брати участі в основній операційній діяльності надавача платіжних послуг або надавач платіжних послуг 6 залучає до таких перевірок інших осіб, які є незалежними від надавача платіжних послуг, на підставі відповідних правових угод,	заклад за акредитованою програмою, акредитація яких здійснюється державними органами України. Для фахівця з вищою освітою - це діплом про набуття кваліфікації за певною спеціальністю. Отже, треба враховувати, що Постанова КМУ від 29 квітня 2015 р. № 266 "Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти" містить лише обмежений перлік спеціальностей, які відповідають визаначенню п.11 прєкту Постанови щодо "захисту інформації та кіберзахисту, інформаційних технологій". Спеціальність, яка			

	сертифікати/дипломи міжнародного та/або державного зразка про здобуття навиків/знань у сферах захисту інформації та кіберзахисту, безпеки переказу коштів та інформаційних технологій.	укладених для цілей перевірки. Такі відповідальні особи повинні мати сертифікати/дипломи ~~міжнародного та/або державного зразка~~ про здобуття навиків/знань у сферах захисту інформації та кіберзахисту, безпеки переказу коштів та інформаційних технологій. **Ці дипломи/сертифікати повинні бути або державного зразка, або видані міжнародними організаціями, які здійснюють сертифікацію відповідних фахівців.**	відповідає визначенню "безпеки переказу коштів" взагалі відсутня. Як відсутня вона і в Міжнародній стандартній класифікації освіти ISCED-F 2013. Термін "диплом міжнародного зразка" взагалі відсутній у термінології українського законодавства і є, скоріш, маркетинговим терміном, ніж юридичним. При цьому є кваліфікаційні сертифікати, наприклад https://www.pcisecuritystandards.org/program_training_and_qualification/ , які не є "сертифікатами міжнародного зразка", але визнаються міжнародними платіжними системами.			
7.	34. Надавач платіжних послуг з обслуговування рахунків не вимагає застосування посиленої	34. Надавач платіжних послуг з обслуговування рахунків не вимагає	Якщо мова іде про базові спеціалізовані інтерфейси відкритого банкінгу, то відповідно	Фізична особа: Дубихвіст Олександр Анатолійович	dubykhvist@gmail.com	23.09.2025 15:42:14

	автентифікації користувачів платіжної послуги **під час надання користувачу доступу до рахунку з використанням засобів дистанційної комунікації** за умови дотримання вимог пунктів 8 та 9 глави 2 розділу I цього Положення **та не розкриття індивідуальної облікової інформації надавачу платіжних послуг з надання відомостей з рахунків і будь-якої іншої інформації, окрім інформації щодо:** **1) залишків на рахунках користувача платіжних послуг;** **2) переліку платіжних операцій, здійснених з рахунків цього користувача платіжних послуг за останні 90 днів.**	застосування посиленої автентифікації користувачів платіжної послуги під час надання користувачу доступу до рахунку з використанням засобів дистанційної комунікації за умови дотримання вимог пунктів 8 та 9 глави 2 розділу I цього Положення та не розкриття індивідуальної облікової інформації надавачу платіжних послуг з надання відомостей з рахунків і будь-якої іншої інформації, окрім інформації щодо: 1) залишків на рахунках користувача платіжних послуг; 2) ~~переліку~~ **історії** платіжних операцій, здійснених з рахунків цього користувача платіжних	до підпункту 2 п.13 розділу II "Положення про відкритий банкінг в Україні", затвердженого Постановою Правління НБУ від 25.07.2025 року №80 *13. НПП з обслуговування рахунку під час надання сторонньому НПП доступу до рахунку користувача через базові спеціалізовані інтерфейси зобов'язаний забезпечувати виконання: 2) запитів щодо надання відомостей з рахунку, а саме щодо суми доступних коштів на рахунку користувача (баланс) та/або історії операцій (за період, що становить не більше ніж **31 календарний день** від поточної дати запиту) за рахунком, наданих користувачем через НПП з надання відомостей з рахунків*			

		послуг ~~за останні 90 днів~~.	*із урахуванням вимог пункту 12 розділу II цього Положення*. Якщо положення Постанови №58 стосуються і комерційних спеціалізованих інтерфейсів, то треба або просто прибрати "за останні 90 днів" (вважаю, що ця редакція більш правильна), або залишити стару редакцію, бо згідно нової, НПП з обслуговування рахунків не зможе пропонувати комерційні сервіси з історії операцій по рахунку з глибиною понад 90 днів без проходження посиленої автентифікації при кожному запиті. Це може бути дуже незручно, особливо для юридичних осіб.			

8.	37-1. Надавач платіжних послуг та інші задіяні у відповідній платіжній операції надавачі платіжних послуг мають право не вимагати застосування посиленої автентифікації користувачів платіжної послуги у разі проведення дистанційної платіжної операції з використанням електронного платіжного засобу, уключаючи токен платіжної картки, на суму, що не перевищує 30 000 гривень, з метою: - сплати податків, зборів та інших обов’язкових платежів до державного та/або місцевих бюджетів, єдиного внеску на загальнообов’язкове державне соціальне страхування, а також визначених контролюючим органом грошових зобов’язань; - погашення (стягнення) податкового боргу,	37-1. Надавач платіжних послуг та інші задіяні у відповідній платіжній операції надавачі платіжних послуг мають право не вимагати застосування посиленої автентифікації користувачів платіжної послуги у разі проведення дистанційної платіжної операції з використанням електронного платіжного засобу, уключаючи токен платіжної картки, на суму, що не перевищує ~~3~~50 000 гривень, з метою: - сплати податків, зборів та інших обов’язкових платежів до державного та/або місцевих бюджетів, єдиного внеску на загальнообов’язкове державне соціальне страхування, а також	Пропонуємо збільшити суму операцій, передбачених цим пунктом, до 50 тисяч гривень.	Юридична особа: АТ "БАНК КРЕДИТ ДНІПРО"	ЄДРПОУ: 14352406, (Irina.Vikhoreva-Sukhorukova@creditdnepr.com)	24.09.2025 12:51:34

	недоїмки зі сплати єдиного внеску на загальнообов'язкове державне соціальне страхування та сплати розстрочених (відстрочених), грошових зобов'язань або податкового боргу платника податків та/або сум єдиного внеску на загальнообов'язкове державне соціальне страхування, або дистанційної платіжної операції з метою оплати житлово-комунальних послуг.	визначених контролюючим органом грошових зобов'язань; - погашення (стягнення) податкового боргу, недоїмки зі сплати єдиного внеску на загальнообов'язкове державне соціальне страхування та сплати розстрочених (відстрочених), грошових зобов'язань або податкового боргу платника податків та/або сум єдиного внеску на загальнообов'язкове державне соціальне страхування**;** ~~, або дистанційної платіжної операції з метою~~ - оплати житлово-комунальних послуг.				
9.	42. Надавач платіжних послуг з обслуговування рахунку не вимагає застосовування посиленої автентифікації платника за умови	42. Надавач платіжних послуг з обслуговування рахунку **має право** не вимага**ти**є застосовування	Оскільки перерахування коштів мж власними рахунками клієнта в межах одного надавача платіжних послуг не	Юридична особа: АТ "БАНК КРЕДИТ ДНІПРО"	ЄДРПОУ: 14352406, (Irina.Vikhoreva-Sukhorukova@creditdnepr.com)	24.09.2025 12:51:34

	дотримання вимог, визначених у пунктах 8 та 9 глави 2 розділу I цього Положення, у разі ініціювання платником кредитового переказу між власними рахунками, що обслуговуються одним надавачем платіжних послуг.	посиленої автентифікації платника ~~за умови дотримання вимог, визначених у пунктах 8 та 9 глави 2 розділу I цього Положення,~~ у разі ініціювання платником кредитового переказу між власними рахунками, що обслуговуються одним надавачем платіжних послуг.	створює жодних ризиків для клієнтів, пропонуємо для таких операцій не вимагати посиленої автентифікації, в тому числі не пов'язувати проведення таких переказів з дотриманням вимог, визначених у пунктах 8 та 9 глави 2 розділу I Положення.			
10.	36. Надавач платіжних послуг, що отримав право на надання нефінансових платіжних послуг, зобов'язаний застосовувати посилену автентифікацію користувачів під час кожного входу користувача до платіжного застосунку.	~~36. Надавач платіжних послуг, що отримав право на надання нефінансових платіжних послуг, зобов'язаний застосовувати посилену автентифікацію користувачів під час кожного входу користувача до платіжного застосунку.~~	Відповідно до п.62 ч.1 ст.1 ЗУ "Про платіжні послуги" *62)* ***платіжний застосунок - програмне забезпечення, що дає змогу користувачу*** *ініціювати платіжну операцію з рахунку платника (у тому числі за допомогою платіжних інструментів) та/****або здійснювати інші операції, передбачені договором з надавачем***	Фізична особа: Дубихвіст Олександр Анатолійович	dubykhvist@gmail.com	25.09.2025 11:16:54

			платіжних послуг; Відповідно підпункті 13 п.34 Постанови №80 34. ***Сторонній НПП зобов'язаний: 13) зазначити в договорі з користувачем умови відповідальності*** *користувача і* ***такого стороннього НПП під час надання нефінансових платіжних послуг користувачу;*** Таким чином, будь яке ПЗ, яке використовується для взаємодії між стороннім НПП та користувачем повинне мати функціонал для посиленої автентифікації, що не є доцільним, бо **Сторонній НПП використовує інофрмацію, яку він отримав від НПП з обслуговуванян рахунку, в спосіб узгоджений з користувачем в**			

			договорі між користувачем і цим Стороннім НПП. Це може бути, наприклад, доступ до інформації або відправка інформації бухгалтерській фірмі, яка обслуговує користувача. Для НПП з ініціювання платежу це взагалі зайва норма, бо цей Сторонній НПП може надавати послуги еквайрінгу в програмному забезпечені торгівця. Пропонуємо видалити цей пункт. Це питання обговорювали на регулярній зустрічі OAG.			
11.	Глава 2 Розділу I: 71. Надавач платіжних послуг має право не застосовувати посилену автентифікацію користувачів платіжної послуги в таких випадках: 1) виконання транскордонної	Глава 2 Розділу I: 71. Надавач платіжних послуг має право не застосовувати посилену автентифікацію користувачів платіжної послуги в таких випадках: 1) виконання транскордонної	Операції по токенізованих картках, зареєстрованих в сервісах ApplePay, Google Pay, проведені з використанням інтернет-ресурсів, здійснюються вже з посиленою автентифікацією.	Юридична особа: ТОВ «НоваПей»	ЄДРПОУ: 38324133, (office@novapay.ua)	26.09.2025 09:10:57

	платіжної операції з використанням реквізитів платіжної картки; 2) виконання платіжної операції в системі S.W.I.F.T.; 3) здійснення платіжної операції з використанням платіжної картки або токена платіжної картки, що ініціюються за допомогою фізичного платіжного пристрою із застосуванням контактної та безконтактної технології.	платіжної операції з використанням реквізитів платіжної картки; 2) виконання платіжної операції в системі S.W.I.F.T.; 3) здійснення платіжної операції з використанням платіжної картки або токена платіжної картки, що ініціюються за допомогою фізичного платіжного пристрою із застосуванням контактної та безконтактної технології; **4) здійснення платіжної операції з використанням токена платіжної картки, що ініціюється в мережі Інтернет.**				
12.	37. Надавач платіжних послуг та інші задіяні у відповідній платіжній операції надавачі платіжних послуг мають	37. Надавач платіжних послуг **з обслуговування рахунку** та інші задіяні у відповідній платіжній	Пропонуємо додати уточнення надавача платіжних послуг, про якого йдеться, або замінити фразу	Юридична особа: ТОВ «НоваПей»	ЄДРПОУ: 38324133, (office@novapay.ua)	26.09.2025 09:10:57

	право не вимагати застосування посиленої автентифікації користувачів платіжної послуги за умови дотримання вимог пунктів 8 та 9 глави 2 розділу I цього Положення, а також одночасного виконання таких умов: 1) сума дистанційної платіжної операції не перевищує 2 000 гривень; 2) загальна сума попередніх платіжних операцій, ініційованих платником з часу застосування останньої посиленої автентифікації користувача платіжної послуги, не перевищує 10 000 гривень або кількість попередніх операцій, ініційованих платником з часу застосування останньої посиленої автентифікації користувача платіжної послуги, не перевищує	операції надавачі платіжних послуг мають право не вимагати застосування посиленої автентифікації користувачів платіжної послуги за умови дотримання вимог пунктів 8 та 9 глави 2 розділу I цього Положення, а також одночасного виконання таких умов: 1) сума дистанційної платіжної операції не перевищує 2 000 гривень; 2) загальна сума попередніх платіжних операцій, ініційованих платником з часу застосування останньої посиленої автентифікації користувача платіжної послуги, не перевищує 10 000 гривень або кількість попередніх операцій, ініційованих платником з часу застосування останньої	«Надавач платіжних послуг та інші задіяні у відповідній платіжній операції надавачі платіжних послуг» фразою «усі надавачі платіжних послуг, задіяні у відповідній платіжній операції» , адже поточне формулювання саме це і означає.			

	п’яти послідовних окремих операцій.	посиленої автентифікації користувача платіжної послуги, не перевищує п’яти послідовних окремих операцій.				
13.	45. Надавач платіжних послуг з обслуговування рахунків має право залучити для проведення посиленої автентифікації користувача платіжної послуги іншого надавача платіжних послуг або технологічного оператора платіжних послуг або оператора платіжної системи.	45. Надавач платіжних послуг з обслуговування рахунків має право залучити для проведення посиленої автентифікації користувача платіжної послуги іншого надавача платіжних послуг або технологічного оператора платіжних послуг або оператора платіжної системи. **Надавач платіжних послуг може врахувати операції з токенами, за якими посилена автентифікація проведена з боку гаманця, в якому закріплено токен, як операції, проведені з**	Доповнити пункт новим абзацом. Численні запити ринку і представників МПС були до Регулятора виключити необхідність додаткової посиленої автентифікації по операціям з токенами, за умови, що автентифікація за допомогою токена і додаткового фактору, вже була виконана гаманцем.	Юридична особа: ТОВ «НоваПей»	ЄДРПОУ: 38324133, (office@novapay.ua)	26.09.2025 09:10:57

		посиленою автентифікацією.				
14.	5(1). Надавач платіжних послуг з обслуговування рахунку має право не вимагати застосування посиленої автентифікації користувача у разі отримання від користувача платіжної інструкції, підписаної кваліфікованим електронним підписом такого користувача	Надавач платіжних послуг з обслуговування рахунку має право не вимагати застосування посиленої автентифікації користувача у разі отримання від користувача платіжної інструкції, підписаної кваліфікованим електронним підписом **або удосконаленим електронним підписом, що базується на кваліфікованому сертифікаті електронного підпису** такого користувача.	Пропонується розширити можливість застосування пункту і для користувачів, які підписують платіжну інструкцію удосконаленим електронним підписом, що базується на кваліфікованому сертифікаті електронного підпису, оскільки це надасть змогу охопити більше коло користувачів. В свою чергу, надавач - в силу запропонованих змін до п.14 - зможе перевірити такий підпис.	Юридична особа: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ АУДИТОРСЬКА ФІРМА ПРАЙСВОТЕРХАУСКУПЕРС (АУДИТ)	ЄДРПОУ: 21603903, (mariia.pichiienko@pwc.com)	26.09.2025 17:10:37
15.	56. Надавач платіжних послуг з обслуговування рахунку повинен щомісяця реєструвати та контролювати для кожного виду дистанційних платіжних операцій, що визначені у додатку до цього	Ми вбачаємо за доцільне додатково розглянути наступні питання: (і) розробити чіткий та стандартизований формат щомісячного звіту щодо коефіцієнта рівня шахрайства;	Періодичність реєстрації та контролю даних щодо коефіцієнта рівня шахрайства значно підвищує вимоги до оперативності моніторингу та звітності та дозволить	Юридична особа: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ АУДИТОРСЬКА ФІРМА ПРАЙСВОТЕРХ	ЄДРПОУ: 21603903, (mariia.pichiienko@pwc.com)	26.09.2025 17:10:37

	Положення нижчезазначені дані...	(ii) визначити (за можливості) основні показники та зміни в коефіцієнті шахрайства, які вимагають негайного внутрішнього розслідування та які конкретні заходи реагування очікуються та винести їх на обговорення з учасниками; (iii) запровадити механізм зворотного зв'язку з надавачами щодо якості та ефективності їхніх щомісячних моніторингових звітів, а також щодо кращих практик у сфері виявлення та запобігання шахрайству.	більш оперативно виявляти та реагувати на шахрайські дії. При цьому, це може суттєво збільшити адміністративне та ресурсне навантаження на надавачів платіжних послуг, особливо якщо процеси моніторингу не повністю автоматизовані. Запропоновані уточнення можуть забезпечити узгодженість даних, полегшить їх збір та обробку, а також підвищить ефективність регуляторного нагляду. Також, визначення показників та змін в коефіцієнті допоможуть надавачам ефективно діяти у критичних ситуаціях.	АУСКУПЕРС (АУДИТ)		
16.	5.1. Надавач платіжних послуг з обслуговування рахунку має право не вимагати застосування посиленої автентифікації	5.1. Надавач платіжних послуг з обслуговування рахунку має право не вимагати застосування	На практиці технологія КЕП використовується як інструмент доступу до рахунків (інструмент авторизації), тому	Юридична особа: Європейська Бізнес Асоціація	ЄДРПОУ: 31811085, (victoria.burdeina@eba.com.ua)	26.09.2025 18:00:31

	користувача у разі отримання від користувача платіжної інструкції, підписаної кваліфікованим електронним підписом такого користувача.	посиленої автентифікації користувача у разі: - отримання від користувача платіжної інструкції, підписаної кваліфікованим електронним підписом такого користувача, **або** **- підтвердження кваліфікованим електронним підписом операції із доступу до рахунку із використанням засобів дистанційної комунації.**	пропонуємо не обмежувати виключення лише платіжними операціями, адже з точку зору надійності використання технології КЕП має висикой рівень довіри і в інших процесах.			
17.	14. Надавач платіжних послуг за результатами процедури посиленої автентифікації користувача платіжної послуги створює код автентифікації. Для створення коду автентифікації надавач платіжних послуг використовує багатоцільові пристрої або програмне забезпечення,	14. Надавач платіжних послуг за результатами процедури посиленої автентифікації користу вача платіжної послуги створює **або покладаєт ься на інших юридичних осіб, з якими встановлені договірні відносини, щодо створення коду автентифікації.** Для створення коду автентифікації надавач	Викласти пункт 14 Глави 4 Постанови № 58 у відповідності до статті 4 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017. Article 4 1. Where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the	Юридична особа: Європейська Бізнес Асоціація	ЄДРПОУ: 31811085, (victoria.burdeina@eba.com.ua)	26.09.2025 18:00:31

	призначене для цілей автентифікації користувача платіжних послуг. Код автентифікації повинен бути стійким до його підробки та стійким до розкриття будь-якого з елементів посиленої автентифікації, з використанням яких цей код було створено. Для забезпечення стійкості коду автентифікації надавач платіжних послуг застосовує такі технологічні рішення, як створення та перевірка справжності одноразових паролів**,** **кваліфікованих електронних підписів, удосконалених електронних підписів з кваліфікованим сертифікатом** чи інші підтвердження з	платіжних послуг використовує багатоцільові пристрої або програмне забезпечення, призначене для цілей автентифікації користувача платіжних послуг. Код автентифікації повинен бути стійким до його підробки та стійким до розкриття будь-якого з елементів посиленої автентифікації, з використанням яких цей код було створено. Для забезпечення стійкості коду автентифікації надавач платіжних послуг застосовує такі технологічні рішення, як створення та перевірка справжності одноразових паролів, кваліфікованих електронних підписів,	authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code. Або врахувати пропозиції наведені Visa, які адаптовані відповідно для надання можливості проведення дистанційних платіжних операцій з використанням технологій Click to Pay, Apple Pay, Google Pay та інших.			

	використанням криптографічних засобів захисту інформації, що містяться в елементах посиленої автентифікації.	удосконалених електронних підписів з кваліфікованим сертифікатом чи інші підтвердження з використанням криптографічних засобів захисту інформації, що містяться в елементах посиленої автентифікації.				
18.	17. Надавач платіжних послуг повинен забезпечити застосування процедури посиленої автентифікації зі створенням коду автентифікації, включаючи такі заходи безпеки: ... 2) кількість невдалих спроб застосування процедури посиленої автентифікації, що можуть здійснюватися послідовно, не повинна перевищувати п’яти **спроб, здійснених з використанням одного**	17. Надавач платіжних послуг повинен забезпечити застосування процедури посиленої автентифікації зі створенням коду автентифікації, включаючи такі заходи безпеки: ... 2) кількість невдалих спроб застосування процедури посиленої автентифікації, що можуть здійснюватися послідовно, не повинна перевищувати п’яти **спроб, здійснених з**	У листі Національного банку від 05.08.2025 № 56-0015/60367 "Про питання щодо проведення посиленої автентифікації" зазначалося, що проєкт змін до Положення № 58 враховуватиме, що зазначені п’ять невдалих спроб мають обчислюватися в розрізі кожного **окремого платіжного інструмента користувача** (а не електронного платіжного засобу). Пропонуємо	Юридична особа: Європейська Бізнес Асоціація	ЄДРПОУ: 31811085, (victoria.burdeina@eba.com.ua)	26.09.2025 18:00:31

	електронного платіжного засобу. Після досягнення граничної кількості невдалих спроб можливість застосування процедури автентифікації повинно бути тимчасово або постійно заблоковано в порядку, визначеному надавачем платіжних послуг;	**використанням одного платіжного інструмента та/або із використанням визначеного засобу дистанційної комунікації**. Після досягнення граничної кількості невдалих спроб можливість застосування процедури автентифікації повинно бути тимчасово або постійно заблоковано в порядку, визначеному надавачем платіжних послуг;	синхронізувати відповідну норму у Проекті змін до Положення НБУ № 58. Також пропонуємо додатково уточнити, що лічильник невдалих спроб застосування процедури посиленої автентифікації може рахуватися у розрізі конкретно **визначеного засобу дистанційної комунікації** надавача платіжних послуг з обслуговування рахунку. Такий підхід дозволить унормувати застосування такого лічильника під час отримання користувачем **доступу до рахунку** за допомогою засобів дистанційної комунікації, адже під час отримання такого доступу до рахунку взагалі не використовується			

			"електронний платіжний засіб"			
19.	17. Надавач платіжних послуг повинен забезпечити застосування процедури посиленої автентифікації зі створенням коду автентифікації, включаючи такі заходи безпеки: ... 4) максимальний час без активності користувача платіжних послуг після проходження посиленої автентифікації та отримання доступу до рахунку з використанням засобів дистанційної комунікації через мережі загального користування не повинен перевищувати десяти хвилин.	17. Надавач платіжних послуг повинен забезпечити застосування процедури посиленої автентифікації зі створенням коду автентифікації, включаючи такі заходи безпеки: ... 4) максимальний час без активності користувача платіжних послуг після проходження посиленої автентифікації та отримання доступу до рахунку з використанням засобів дистанційної комунікації через мережі загального користування не повинен перевищувати десяти хвилин. **Для користувача юридичної особи або фізичної особи-підприємця**	Пропонуємо для користувача юридичної особи або фізичної особи-підприємця встановити більш тривалий час без активності користувача, зважаючи на те, що такий користувач (або його уповноважений представник) більший час перебуває у системі дистанційної комунікації, ніж користувач фізична - особа. Наприклад: бухгалтер підприємства може перебувати у системі 8-10 годин (в межах власного робочого дня) перемикаючись між інтернет-банкінгом та бухгалтерськими програмами. Згідно попереднього опитування користувачів великого корпоративного	Юридична особа: Європейська Бізнес Асоціація	ЄДРПОУ: 31811085, (victoria.burdeina@eba.com.ua)	26.09.2025 18:00:31

		максимальний час без активності після проходження посиленої автентифікації та отримання доступу до рахунку з використанням засобів дистанційної комунікації через мережі загального користування не повинен перевищувати шістдесяти хвилин	сегменту 10 хвилин без активності це дуже малий час, який призводить до частої переавторизації в системі протягом дня.			
20.	44. Надавач платіжних послуг з обслуговування рахунків не вимагає застосування посиленої автентифікації користувачів платіжної послуги за дебетовим переказом за умови отримання згоди платника на виконання такої платіжної операції або в разі здійснення дебетового переказу стягувачем.	44. Надавач платіжних послуг з обслуговування рахунків не вимагає застосування посиленої автентифікації користувачів платіжної послуги за дебетовим переказом за умови отримання згоди платника **(у тому числі, якщо така згода надається користувачем торговцю)** на виконання такої платіжної операції або	Пропонуємо врегулювати ситуації, коли клієнт надає згоду на підключення регулярного платежу за надані товари або послуги з його власного рахунку через мобільний або веб-додаток торговця. При цьому, з огляду на те, що такий додаток не належить надавачу платіжних послуг з обслуговування рахунку, такий надавач технічно не має	Юридична особа: Європейська Бізнес Асоціація	ЄДРПОУ: 31811085, (victoria.burdeina@eba.com.ua)	26.09.2025 18:00:31

		в разі здійснення дебетового переказу стягувачем.	можливості провести посилену автентифікацію.			
21.	45. Надавач платіжних послуг з обслуговування рахунків має право залучити для проведення посиленої автентифікації користувача платіжної послуги іншого надавача платіжних послуг або технологічного оператора платіжних послуг або оператора платіжної системи.	45. Надавач платіжних послуг з обслуговування рахунків має право залучити для проведення посиленої автентифікації користувача платіжної послуги іншого надавача платіжних послуг або технологічного оператора платіжних послуг або оператора платіжної системи **або інших юридичних осіб, з якими встановлені договірні відносини.**	Пропозиції наведені Visa адаптовані відповідно для надання можливості проведення дистанційних платіжних операцій з використанням технологій Click to Pay, Apple Pay, Google Pay та інших.	Юридична особа: Європейська Бізнес Асоціація	ЄДРПОУ: 31811085, (victoria.burdeina@eba.com.ua)	26.09.2025 18:00:31